UNIVERSIDAD DE LA RIOJA

TRABAJO FIN DE ESTUDIOS

Título

La aritmética de los números cuadráticos

Autor/es

PEIO ARDAIZ GALE

Director/es

JESÚS ANTONIO LALIENA CLEMENTE

Facultad

Facultad de Ciencia y Tecnología

Titulación

Grado en Matemáticas

Departamento

MATEMÁTICAS Y COMPUTACIÓN

Curso académico

2018-19

publicaciones.unirioja.es
E-mail: publicaciones@unirioja.es

UNIVERSIDAD DE LA RIOJA

Facultad de Ciencia y Tecnología

TRABAJO FIN DE GRADO

Grado en Matemáticas

La aritmética de los números cuadráticos

Realizado por:

Peio Ardaiz Galé

Tutelado por:

Jesús Antonio Laliena Clemente

Logroño, julio, 2019

La aritmética de los números cuadráticos

Índice

Resumen

En este trabajo vamos a estudiar la aritmética en los cuerpos cuadráticos, es decir, cuerpos de la forma $\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$. Para ello, estudiaremos unos subanillos de los cuerpos cuadráticos análogos a $\mathbb{Z} \subset \mathbb{Q}$ conocidos como anillos de enteros cuadráticos. Intentaremos factorizar los elementos de estos anillos de enteros cuadráticos de manera análoga a los enteros en $\mathbb{Z}$. El estudio se realizará desde un punto de vista principalmente algebraico.

Empezaremos dando un repaso a la teoría de anillos y a la de retículos, que serán nuestras dos principales herramientas a la hora de trabajar con los cuerpos cuadráticos. Obtendremos dos resultados principales. En primer lugar, que todo ideal de un anillo de enteros cuadráticos se factoriza de manera única en producto de ideales primos. En segundo lugar, que los enteros cuadráticos se factorizarán de manera única si y solo si el anillo de enteros en el que están contenidos es un dominio de ideales principales (DIP). Además, definiremos un grupo abeliano, conocido como grupo de clases de ideales, que nos indicará, según su tamaño, cómo de lejos está un anillo de enteros cuadráticos de ser un DIP.

Abstract

In this paper we will study the arithmetic of quadratic fields, i.e., fields of the form $\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$. For that purpose, we will work in some subrings of these quadratic fields analogous to $\mathbb{Z} \subset \mathbb{Q}$, known as rings of integers of $\mathbb{Q}[\sqrt{D}]$. We will try to factorize elements of these subrings in an analogous way to that of integers in $\mathbb{Z}$. We will work, mainly, from an algebraic point of view.

First, we will speak briefly about ring theory and lattices. These will be our main tools when working with quadratic fields. We will obtain two main results. Firstly, we will prove that each ideal of the ring of integers can be written, esentially uniquely, as a product of prime ideals. Secondly, we will prove that quadratic integers have unique factorization if and only if its ring of integers is a PID. Additionally, we will define an abelian group called the ideal class group; it will show us, depending on its size, how far is a ring of integers from being a PID.

Introducción

El estudio de los cuerpos cuadráticos y su aritmética se inicia, al igual que tantas otras ramas de estudio matemáticas, con un intento de de resolver el Último Teorema de Fermat. En concreto, fue Gauss quien, para demostrar dicho teorema cuando $n = 3$, utilizó los anillos de enteros cuadráticos. La idea de Gauss de utilizar los números complejos para tratar de encontrar una demostración supuso una auténtica revolución. Como bien dijo Hadamard "El camino más corto entre dos verdades del campo real pasa con frecuencia por el campo complejo" (ver, por ejemplo, página 18 de Introducción de [3]). Posteriormente, numerosos matemáticos, entre los que destacan Dirichlet, Lebesgue, Lamé o Cauchy, siguieron el camino de los anillos de enteros ciclotómicos marcado por Gauss para avanzar en la solución del teorema para distintos valores de n.

El 1 de marzo de 1847, Lamé presenta en la Academia de Ciencias de París lo que él creía que era la demostración definitiva del Último Teorema de Fermat. Pero Liouville, a quién Lamé atribuía la idea principal de su demostración, dudaba de la corrección de la misma. Sus principales objeciones se basaban en que Lamé había asumido la existencia de factorización en los anillos de enteros ciclotómicos, lo cual estaba lejos de ser obvio. Cauchy también se interesó por este intento de demostración. Tanto Cauchy como Lamé trataron de probar que los anillos de enteros ciclotómicos poseían la propiedad de factorización deseada. Lamé aseguraba haber probado que todo elemento de tales anillos se descomponía en irreducibles, y que en los casos que conocía esas descomposiciones eran equivalentes, pero en realidad no lo consiguió probar.

Sea abría por tanto un nuevo campo de estudio, la factorización en los anillos de enteros, y con él distintas preguntas: ¿podemos asumir en todos ellos las propiedades de factorización presentes en $\mathbb{Z}$?, ¿es equivalente hablar de números primos e irreducibles, o debemos dar una definición para cada uno?, ¿en caso de no tener las propiedades de factorización deseadas, podremos recuperarlas mediante la introducción de algún nuevo objeto matemático?.

La discusión entre Lamé y Liouville fue zanjada por Kummer. En una carta leída por Liouville en la Academia de Ciencias de París el 24 de mayo del mismo año, aseguraba que las objeciones de este último eran acertadas. Con la carta, Kummer incluía una memoria que había publicado años antes, en la que demostraba que, en efecto, los anillos de enteros ciclotómicos no poseen las propiedades de factorización deseadas. Sin embargo, aseguraba que se podía recuperar la factorización introduciendo un nuevo tipo de números complejos a los que denominaba *números complejos ideales*, más tarde conocidos simplemente como ideales. Los ideales han sido posteriormente una de las herramientas más importantes de las matemáticas. Este concepto, perteneciente a la teoría de anillos, se utiliza, por ejemplo, para resolver sistemas de ecuaciones polinómicas (ver la teoría de bases de Gröbner, en [2]), omnipresentes en cualquier rama científica (matemáticas, física, economía, biología...).

Kummer consiguió probar la factorización única de ideales en los anillos de enteros ciclotómicos e inventó una forma de comprobar si un anillo de enteros era un dominio de factorización única, el grupo de clases de ideales. De esta forma, Kummer consiguió dar un impulso enorme a la resolución del Último Teorema de Fermat.

En el siguiente trabajo se probarán los dos resultados principales de Kummer en el caso de los anillos de enteros cuadráticos. Para ello, nos valdremos principalmente de dos herramientas; la teoría de anillos, y los retículos. Estos últimos nos dan una forma de representar

los anillos de enteros cuadráticos en el plano, además de ampliar la teoría estándar de reducción gaussiana a matrices con entradas en $\mathbb{Z}$, lo que nos facilitará en gran medida los cálculos con ideales.

A continuación se expondrá un breve resumen de los contenidos.

Capítulo 1: Generaliza, en la medida de lo posible, la aritmética en $\mathbb{Z}$ a varios cuerpos cuadráticos. Los ejemplos se han elegido de forma que se pueda apreciar la variedad de nuevos fenómenos que aparecen en la teoría de números algebraica.

Capítulo 2: Ofrece un breve repaso sobre la teoría de anillos que será necesario utilizar a lo largo del trabajo.

Capítulo 3: Se definen los retículos y se utilizan para ampliar la reducción gaussiana a matrices con entradas en $\mathbb{Z}$.

Capítulo 4: Se trata del capítulo principal del trabajo. En él se desarrolla la teoría de números algebraica en un cuerpo cuadrático genérico, y culmina con la prueba de la factorización única de ideales.

Capítulo 5: Prueba la finitud del grupo de clases de ideales y aporta varios ejemplos acerca de cómo calcular y clasificar dicho grupo.

Apéndice: Ofrece una visión rápida de la relación entre formas cuadráticas y la aritmética de los cuerpos cuadráticos. Se ilustra mediante un ejemplo el principal teorema de este capítulo, que muestra la existencia de un isomorfismo entre *el grupo de clases estrictas de ideales*, clases de equivalencia de formas cuadráticas y clases de equivalencia de números cuadráticos.

Este trabajo está basado en el libro *Algebraic theory of quadratic numbers*, de Mak Trifković [7], del cual se han elegido varias partes que han sido traducidas y resumidas. Además, al final de cada capítulo de esta memoria se incluyen varios ejercicios que propone el libro, ya sea para ilustrar algún ejemplo o para completar ciertos aspectos de la teoría que el libro deja para el lector. Los datos históricos que aparecen al inicio de esta introducción han sido extraídos, en parte, del libro *El reto de Fermat*, de Ángel del Río Mateos [4]. Otro libro divulgativo en el que se pueden encontrar múltiples aplicaciones de la teoría desarrollada para resolver el Último Teorema de Fermat, así como distintas historias y anécdotas relacionadas con su resolución, es *El enigma de Fermat*, de Simon Singh [6].

1. Motivación y ejemplos

El siguiente tema contiene un repaso de Teoría de Números elemental y distintos ejemplos de cuerpos cuadráticos que nos servirán de motivación para lo que se va a estudiar a lo largo del trabajo.

1.1. Teoría de números elemental

¿Podemos expresar un número primo como suma de dos cuadrados? Rápidamente observamos que unos si y otros no:

$$p = a^2 + b^2 : 2, 5, 13, 17, 29, 37...$$
$$p \neq a^2 + b^2 : 3, 7, 11, 19, 23, 31...$$

¿Se aprecia algún patrón? Esta pregunta fue propuesta por Fermat en el Siglo XVII, y es un ejemplo de la necesidad de estudiar divisibilidad, primos y factorización en cuerpos más grandes que $\mathbb{Z}$. El hecho de que un primo se pueda escribir como suma de dos cuadrados implica que:

$$p = a^2 + b^2 = (a + bi)(a - bi), \text{ con a, b} \in \mathbb{Z}$$

Mostrando que p tiene una factorización no trivial en el conjunto

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

El Teorema de Factorización Única, el Algoritmo de la División y el Algoritmo de Euclides, ampliamente conocidos, dan respuesta a las cuestiones de factorización y divisibilidad en $\mathbb{Z}$, ¿se podrán encontrar resultados equivalentes para conjuntos del tipo $\mathbb{Z}[i]$? Vamos a recordar a continuación estos tres resultados y también el Lema de Euclides.

Teorema 1.1 (Factorización Única en $\mathbb{Z}$)**.** *Todo entero distinto de* 0 *y* ± 1 *se puede escribir como un producto de primos de manera única, salvo permutación de factores primos y cambio de signos.*

Proposición 1.1 (Algoritmo de la División)**.** *Dados* $a, b \in \mathbb{Z}, b \neq 0$*, existen* q, r *únicos de forma que*

$$a = qb + r; \quad 0 \leq r < |b|$$

Proposición 1.2 (Algoritmo de Euclides)**.** *Dados* $a, b \in \mathbb{Z}$*, con al menos uno de los dos distinto de 0. El máximo común divisor de a y b satisface la siguiente condición: Para cualquier divisor común c de a y b, se tiene que* $c \mid$ *m.c.d.(a,b). Es más, existen* $r, s \in \mathbb{Z}$ *tales que m.c.d.(a,b)=ra+sb.*

Proposición 1.3 (Lema de Euclides)**.** *Para cualquier primo p y cualquier* $a,b \in \mathbb{Z}$*,* $p|ab$ *implica* $p|a$ *o* $p|b$*.*

Trataremos de buscar un análogo a (1.1) para los números cuadráticos.

Definición 1.1 (Número cuadrático)**.** Un **número cuadrático** es aquel que es solución de la ecuación $ax^2 + bx + c$ con $a, b, c \in \mathbb{Z}$. A menudo tendremos que resolver esa ecuación en módulo n.

Definición 1.2 (Símbolo de Legendre)**.** Sea p un primo positivo impar, $a \in \mathbb{Z}$. Decimos que "a es un cuadrado mod p" cuando a $\equiv b^2 \pmod{p}$ para algún b $\in \mathbb{Z}$. Definimos el **símbolo de Legendre** como

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si a es un cuadrado mod p distinto de 0} \\ -1 & \text{si a no es un cuadrado mod p} \\ 0 & \text{si p} \mid a \end{cases}$$

El símbolo de Legendre posee varias propiedades que nos facilitarán su cálculo cuando trabajemos módulo un entero positivo.

Teorema 1.2. *Sean $a, b \in \mathbb{Z}$, y $p, q \in \mathbb{N}$ primos positivos distintos e impares. El símbolo de Legendre satisface las siguientes propiedades:*

(a) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

(b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(c) Si $a \equiv b \pmod{p}$*, entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(d) $\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) \text{ si } p \equiv q \equiv 3 \pmod{4} \\ \left(\frac{q}{p}\right) \text{ en otro caso} \end{cases}$

(e) $\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ si } p \equiv 1 \pmod{4} \\ -1 \text{ si } p \equiv 3 \pmod{4} \end{cases}$

(f) $\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ si } p \equiv \pm 1 \pmod{8} \\ -1 \text{ si } p \equiv \pm 3 \pmod{8} \end{cases}$

La propiedad (d) es normalmente conocida como Ley de Reciprocidad Cuadrática. El denominador en el Símbolo de Legendre debe ser un primo positivo.

Una vez explicada esta noción básica de Teoría de Números, podemos proceder con el estudio de la aritmética de los números cuadráticos. Teniendo en cuenta la Definición 1.1, la expresión de un número cuadrático viene dada por

$$x = \frac{-b \pm \sqrt{D}}{2a}, \text{ donde } D = b^2 - 4ac$$

La formula cuadrática anterior sugiere que debemos trabajar en un cuerpo que contenga a $\sqrt{D}$, por eficiencia, deberíamos elegir también el más pequeño de todos ellos.

Definición 1.3 (Cuerpo cuadrático)**.** Definimos un **cuerpo cuadrático** como:

$$F = \mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$$

Es fácil comprobar que el conjunto anterior es un cuerpo.

Siempre podemos dividir en un cuerpo, por tanto, para encontrar cuestiones interesantes sobre divisibilidad deberemos trabajar en un subanillo $\mathcal{O} \subset F$ análogo a $\mathbb{Z} \subset \mathbb{Q}$. Como veremos a lo largo del trabajo, no siempre existe una factorización única en elementos "primos" en estos subanillos, pero sí que obtendremos los siguientes resultados:

- Cada *ideal* de $\mathcal{O}$ puede ser escrito de manera única como producto de ideales primos.
- Definiremos un grupo abeliano que nos mostrará, según su tamaño, como de lejos está $\mathcal{O}$ de poseer factorización única (este caso se dará cuando el grupo sea trivial). Se probará que este grupo es finito, por tanto nunca se estará demasiado lejos de tener factorización única.

1.2. $\mathbb{Q}[i]$ y los Enteros de Gauss

En este apartado trabajaremos con $\mathbb{Q}[i]$ y $\mathbb{Z}[i]$, los elementos de este últimmo conjunto se conocen como Enteros de Gauss. Veremos que en este caso sí se da la factorización única.

Definición 1.4 (Unidad)**.** Llamamos **unidad de un anillo** R a los elementos del anillo que poseen inverso multiplicativo. El conjunto de las unidades forma un grupo multiplicativo denotado R^X.

Definición 1.5 (Norma)**.** La **norma** de $\alpha = a + bi \in \mathbb{Q}[i]$ es $N\alpha = \alpha\bar{\alpha} = a^2 + b^2 \in \mathbb{Q}$

Teniendo en cuenta estas dos definiciones, es fácil probar los siguientes resultados.

Proposición 1.4. *Sean* $\alpha, \beta \in \mathbb{Q}[i]$*,* $N(\alpha\beta) = N\alpha \cdot N\beta$

Demostración. $\mathrm{N}(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = \mathrm{N}\alpha\mathrm{N}\beta$. □

Proposición 1.5. *Sea* $\epsilon \in \mathbb{Z}[i]$*, entonces* ϵ *es una unidad si y solo si* $N\epsilon = \pm 1$

Demostración. Si $\epsilon \in \mathbb{Z}[i]^\times$, entonces existe $\nu \in \mathbb{Z}[i]$ tal que $\epsilon\nu = 1$. Tomando normas tenemos que $\mathrm{N}\epsilon\mathrm{N}\nu = 1$, luego $\mathrm{N}\epsilon \in \mathbb{Z}^\times$. Inversamente, si $\mathrm{N}\epsilon = \epsilon\bar{\epsilon} = \pm 1$, tenemos que $\epsilon^{-1} = \pm\bar{\epsilon} \in \mathbb{Z}[i]$. □

Proposición 1.6. *El grupo de unidades de* $\mathbb{Z}[i]$*, es* $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

Demostración. Sea $\epsilon = a + bi$, con $a, b \in \mathbb{Z}$. Por la Proposición anterior, ϵ es una unidad si y solo si $\mathrm{N}\epsilon = a^2 + b^2 = \pm 1$. Por tanto (a, b) es $(\pm 1, 0)$ o $(0, \pm 1)$. □

El Algoritmo de la División en $\mathbb{Z}$ nos permite dividir obteniendo un resto que es menor que el valor absoluto del divisor. Cambiando el valor absoluto por la norma, obtenemos un algoritmo de la división en $\mathbb{Z}[i]$.

Proposición 1.7. *Dados* $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$ *existen* $\kappa, \lambda \in \mathbb{Z}[i]$ *tales que* $\alpha = \kappa\beta + \lambda$*, con* $N\lambda < N\beta$*.*

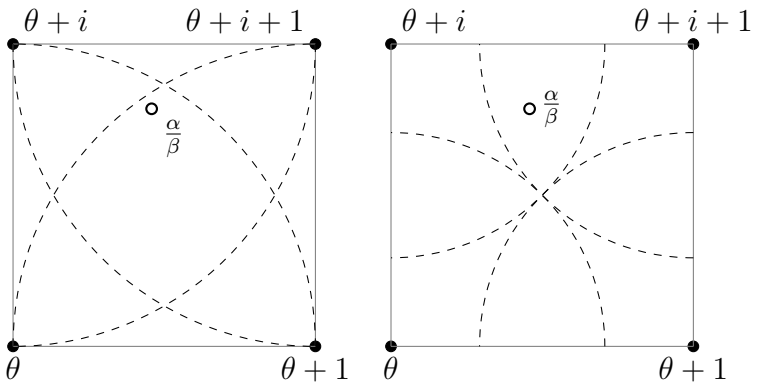

Figura 1: α/β siempre está dentro de al menos uno de los círculos de radio 1 centrados en los puntos más cercanos del retículo (*izquierda*). De hecho, siempre hay un punto en $\mathbb{Z}[i]$ cuya distancia a α/β es a lo sumo $\sqrt{2}/2$ (*derecha*).

Demostración. Las traslaciones del cuadrado formado por los elementos de $\{0, 1, i, 1+i\} \subset \mathbb{Z}[i]$ teselan por completo el plano complejo. Como podemos ver en la Figura 1, la traslación que contiene a α/β queda completamente cubierta por los cuatro círculos de radio 1 centrados en sus vértices. Tomamos como κ cualquier vértice cuya distancia a α/β es menor que 1, es decir, $\mathrm{N}(\alpha/\beta - \kappa) < 1$. Multiplicando por $\mathrm{N}\beta$ tenemos que $\mathrm{N}(\alpha - \kappa\beta) <\mathrm{N}\beta$, y tomamos $\lambda = \alpha - \kappa\beta$. Es posible que κ pueda tener valores distintos; la Proposición no hace ninguna afirmación sobre unicidad. □

Definición 1.6 (Elemento irreducible)**.** Un elemento $\pi \in \mathbb{Z}[i]$ que no sea una unidad, se dice **irreducible** si $\pi = \alpha\beta$ implica que $\alpha \in \mathbb{Z}[i]^\times$ o $\beta \in \mathbb{Z}[i]^\times$.

Vamos a intentar probar que todo elemento de $\mathbb{Z}[i]$ se factoriza en irreducibles, y que cualquiera de sus factorizaciones son equivalentes en el siguiente sentido.

Definición 1.7. Sea $\alpha = \pi_1\pi_2\cdots\pi_r = \pi'_1\pi'_2\cdots\pi'_{r'}$, dos factorizaciones de α en elementos irreducibles de $\mathbb{Z}[i]$. Decimos que las dos **factorizaciones** son **equivalentes** si se cumple que:

(a) $r = r'$

(b) Existe una permutación $\sigma : \{1, ..., r\} \to \{1, ..., r\}$, y unidades $\epsilon_i \in \mathbb{Z}[i]^\times$, tales que $\pi'_i = \epsilon_i\pi_{\sigma(i)}$, para todo $i \in \{1, ..., r\}$

Es decir, dos factorizaciones son equivalentes si una se puede obtener de la otra reordenando sus factores y multiplicando cada uno de ellos por una unidad.

Definición 1.8 (Máximo común divisor)**.** Sean $\alpha, \beta \in \mathbb{Z}[i]$, al menos uno de los dos distinto de cero. Un **máximo común divisor** de α y β es cualquier $\delta \in \mathbb{Z}[i]$ cumpliendo que:

(a) $\delta \mid \alpha$ y $\delta \mid \beta$

(b) Para todo $\gamma \in \mathbb{Z}[i]$, si $\gamma \mid \alpha$ y $\gamma \mid \beta$, entonces $\gamma \mid \delta$

El m.c.d. no está definido de manera única, si δ y δ' satisfacen la definición, la condición (b) muestra que $\delta' = \epsilon\delta$ para cierta unidad ϵ.

Proposición 1.8. *Sean $\alpha, \beta \in \mathbb{Z}[i]$, al menos uno distinto de 0. Entonces existe un m.c.d. δ de α y β. Cualquiera de esos δ se puede escribir como $\delta = \varphi\alpha + \theta\beta$ para ciertos $\varphi, \theta \in \mathbb{Z}[i]$.*

La anterior proposición invita a buscar δ en el conjunto

$$I = \{\mu\alpha + \nu\beta : \mu, \nu \in \mathbb{Z}[i]\}$$

Vamos a probar que I es el conjunto de todos los Enteros de Gauss divisibles por cierto $\delta \in I$. Es fácil ver que I es cerrado respecto a las suma de elementos de I y que absorbe multiplicaciones por elementos de $\mathbb{Z}[i]$.

Lema 1.1. *Sea $\delta \neq 0$ un elemento de I de norma mínima (podemos garantizar su existencia ya que $\{N(\alpha) : \alpha \in I\}$ es un conjunto de $\mathbb{N}$ y por tanto bien ordenado). Entonces $I = \mathbb{Z}[i] \cdot \delta$, es decir, el conjunto de todos los multiplos de δ.*

Demostración. Lo probaremos por doble contenido. Dado que $\delta \in I$, la absorción de multiplaciones implica que $\mathbb{Z}[i] \cdot \delta \subseteq I$. Ahora queda probar que cualquier $\eta \in I$ es divisble por δ. Sabemos por la Proposición 1.7 que existen $\kappa, \lambda \in \mathbb{Z}[i]$ tales que $\eta = \kappa\delta + \lambda$ con $N\lambda < N\delta$. Por ser I cerrado respecto a sumas y absorber productos se tiene que $\lambda = \eta - \kappa\delta \in I$. Si $\lambda \neq 0$ tenemos un elemento de I distinto de δ de norma menor, contradiciendo la elección de δ, por tanto $\lambda = 0$ y $\delta \mid \eta$. □

Demostración de la proposición (1.8). Es fácil ver que el δ del Lema 1.1 es un m.c.d. de α y β. □

A partir de esta momento, la demostración de la Factorización Única en $\mathbb{Z}[i]$ se hace siguiendo los mismos pasos que para $\mathbb{Z}$.

Proposición 1.9 (Lema de Euclides para los Enteros de Gauss)**.** *Para cualquier elemento irreducible $\pi \in \mathbb{Z}[i]$ y cuales quiera $\alpha, \beta \in \mathbb{Z}[i]$, $\pi \mid \alpha\beta$ implica $\pi \mid \alpha$ o $\pi \mid \beta$.*

Teorema 1.3 (Factorización Única en los Enteros de Gauss)**.** *Cualquier elemento de $\mathbb{Z}[i]$ que no sea una unidad es un producto de elementos irreducibles. Las distintas factorizaciones que pueda haber son equivalentes.*

Proposición 1.10. *Sea $\alpha \in \mathbb{Z}[i]$. Si $N\alpha$ es primo en $\mathbb{Z}$, entonces α es irreducible.*

Demostración. $\alpha = \beta\gamma$ implica $p = N\alpha = N\beta \cdot N\gamma$, por ser p primo, $N\beta = \pm 1$, por tanto β es una unidad. □

Con el conocimiento que tenemos sobre $\mathbb{Z}[i]$ ya podemos constestar a la pregunta planteada por Fermat:

Teorema 1.4. *Sea $p \in \mathbb{N}$ un primo impar, entonces p es una suma de dos cuadrados si y sólo si $p \equiv 1 \pmod 4$.*

Demostración. Supongamos que existen $a, b \in \mathbb{Z}$ tales que $p = a^2 + b^2$. Como los únicos cuadrados en módulo 4 son 0 y 1, y p es impar, se tiene que $p \equiv 1 \pmod 4$. Probemos la otra implicación, sea un primo $p \equiv 1 \pmod 4$. Por la propiedad del símbolo de Legendre, $\left(\frac{-1}{p}\right) = 1$ si $p \equiv 1 \pmod 4$, así que existe $n \in \mathbb{Z}$ tal que $n^2 \equiv -1 \pmod p$, es decir, $p \mid n^2+1$. Factorizando $n^2 + 1$ en $\mathbb{Z}[i]$, tenemos $p \mid (n + i)(n - i)$. Claramente, $p \nmid (n \pm i)$, ya que si lo hiciera, el cociente, perteneciente a los Enteros de Gauss, tendría parte imaginaria $\pm 1/p$. En consecuencia y teniendo en cuenta el Lema de Euclides, p, visto como un elemento de $\mathbb{Z}[i]$, no puede ser irreducible . Tomamos una factorización no trivial $p = \alpha\beta$ con $N\alpha \neq 1 \neq N\beta$. Tomando normas $p^2 = Np = N\alpha \cdot N\beta$, por tanto $N\alpha = N\beta = p$. Poniendo $\alpha = a + bi$ tenemos que $p = a^2 + b^2$. □

Teorema 1.5. *Un elemento $\pi \in \mathbb{Z}[i]$ es irreducible si y sólo si una de las siguientes condiciones se cumple:*

(a) $N\pi = p$ es un primo en $\mathbb{N}$, necesariamente $p \equiv 1 \pmod 4$ o $p = 2$.

(b) $\pi = \epsilon p$, $\epsilon \in \mathbb{Z}[i]^\times$ y $p \in \mathbb{N}$ un primo congruente con 3 (mód 4)

Demostración. Veamos que los elementos de (a) y (b) son irreducibles. El caso (a) se deduce de la Proposición 1.10 y el Teorema 1.4. Para (b), supongamos que $p = \alpha\beta$, con $\alpha, \beta \notin \mathbb{Z}[i]^\times$. La prueba del Teorema 1.4 muestra que $N\alpha = N\beta = p$. Pero entonces tendríamos que $p \equiv 0, 1$ o $2 \pmod 4$, contradiciendo nuestra suposición de que $p \equiv 3 \pmod 4$. A la inversa, supongamos que $\pi \in \mathbb{Z}[i]$ es irreducible. Dado que $\pi \mid \pi\bar{\pi} = N\pi$, el Lema de Euclides para $\mathbb{Z}[i]$ garantiza que π divide a algún factor primo p de $N\pi \in \mathbb{Z}$. Por tanto $N\pi \mid Np = p^2$, lo que ocurre si:

(a) $N\pi = p$.

(b) $N\pi = p^2$. Dado que π divide a p, $\eta = p/\pi$ está en $\mathbb{Z}[i]$ y tiene norma

$$N\eta = \frac{Np}{N\pi} = \frac{p^2}{p^2} = 1.$$

Esto significa que $\epsilon = \eta^{-1}$ es una unidad y $\pi = \epsilon p$ como se pretendía. Veamos que $p \equiv 3 \pmod 4$. Si p fuera $\equiv 1 \pmod 4$, entonces por el Teorema 1.4 tendríamos que $p = a^2 + b^2 = N\pi'$, para $\pi' = a + bi$ necesariamente irreducible por la Proposición 1.10. Por tanto π' y π son dos factores irreducibles de p distintos, dado que sus normas son distintas. Por tanto π' divide a una unidad $\eta = p/\pi$, lo que es una contradicción.

□

1.3. Enteros Cuadráticos

La aritmética en $\mathbb{Z}[i]$ es paralela a la $\mathbb{Z}$ debido a que ambos anillos tienen un algoritmo de la división. La prueba de este algoritmo en $\mathbb{Z}[i]$ se desprende directamente del hecho de que los Enteros de Gauss son vértices de una teselación regular del plano complejo por paralelogramos. Ese tipo de subconjunto del plano se conoce como retículo.

Definición 1.9. Un **retículo** en $\mathbb{C}$ es un conjunto de la forma

$$\mathbb{Z}\kappa + \mathbb{Z}\lambda = \{m\kappa + n\lambda : m, n \in \mathbb{Z}\}$$

donde $\kappa, \lambda \in \mathbb{C}\backslash 0$ no son colineales, es decir, $\lambda/\kappa \notin \mathbb{R}$.

Trabajaremos más a fondo con los retículos en el Capítulo 3.

¿Que números cuadráticos, además de $\mathbb{Z}[i]$, podemos considerar como una generalización de $\mathbb{Z}$? Siguiendo el ejemplo de $\mathbb{Z}[i]$, podemos buscar subanillos de $\mathbb{C}$ que también sean retículos. Dado que buscamos subanillos unitarios, nos interesan retículos de la forma $\mathbb{Z}+\mathbb{Z}\alpha$ que sean cerrados por multiplicaciones. Esto ocurre si y sólo si $\alpha^2 \in \mathbb{Z}+\mathbb{Z}\alpha$, dando el siguiente criterio:

$$\mathbb{Z} + \mathbb{Z}\alpha \text{ es un anillo} \Leftrightarrow \alpha^2 + a\alpha + b = 0 \text{ para ciertos } a, b \in \mathbb{Z},$$

y sugiriendo la siguiente definición.

Definición 1.10 (Entero Cuadrático)**.** Un **entero cuadrático** es un $\alpha \in \mathbb{C}$ que es raíz del polinomio $x^2 + ax + b$ para ciertos $a, b \in \mathbb{Z}$.

La ampliación de $\mathbb{Z}$ por i para construir $\mathbb{Z}[i]$ se generaliza para cualquier anillo R y cualquier α elemento de un anillo más grande o variable. El anillo más pequeño conteniendo a R y a α se denota $R[\alpha]$. Es fácil ver que las propiedades de clausura de los anillos implican que

$$R[\alpha] = \{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 : n \in \mathbb{Z}_{\geq 0}, a_k \in R \text{ para todo } 0 \leq k \leq n\}$$

Si α no es raíz de ningún polinomio con coeficientes en R, entonces $R[\alpha]$ es el anillo de polinomios en la variable α con coeficientes en R.

Si α satisface la ecuación $\alpha^2+a\alpha+b = 0$ con coeficientes en R, tenemos que $\alpha^2 = -b-a\alpha$, $\alpha^3 = \alpha\alpha^2 = -b\alpha - a\alpha^2 = ab + (a^2 - b)\alpha$, etc. Dado que el coeficiente director de la ecuación es 1, toda potencia de α, y en consecuencia, todo elemento de $R[\alpha]$, es una combinación linear de 1 y α con coeficientes en R (combinación R-lineal). En particular $\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha$.

1.4. $\mathbb{Q}[\sqrt{-3}]$ y los Enteros de Eisenstein

El concepto de los enteros cuadráticos nos permite estudiar la aritmética en $\mathbb{Q}[\sqrt{-3}]$.

Proposición 1.11. *El conjunto de todos los enteros cuadráticos en $\mathbb{Q}[\sqrt{-3}]$ es $\mathbb{Z}+\mathbb{Z}\omega$, con $\omega = (1+\sqrt{-3})/2$. En concreto, este conjunto es un anillo, llamado anillo de los enteros de Eisenstein.*

Demostración. El único polinomio cuadrático mónico con raíz $a + b\sqrt{-3}$ es

$$(x - (a + b\sqrt{-3}))(x - (a - b\sqrt{-3})) = x^2 - 2ax + (a^2 + 3b^2).$$

Sea $\mathcal{O}$ el conjunto de todos los enteros cuadráticos en $\mathbb{Q}[\sqrt{-3}]$. Por la definición de entero cuadrático, $a + b\sqrt{-3} \in \mathcal{O}$ si y sólo si $2a = m$, $a^2 + 3b^2 = k$ para ciertos $m, k \in \mathbb{Z}$. Poniendo $b = r/s$ con $m.c.d.(r, s) = 1$. Entonces $12r^2/s^2 = 12b^2 = 4k - m^2 \in \mathbb{Z}$, lo que implica que $s^2 \mid 12$. Eso ocurre solo si $s = 1$ o $s = 2$.

En cualquier caso podemos escribir $a = m/2$ y $b = n/2$ para ciertos $m, n \in \mathbb{Z}$. Entonces $m^2/4 + 3n^2/4 = k \in \mathbb{Z}$, lo que implica $m^2 + 3n^2 \equiv m^2 - n^2 \equiv 0 \pmod 4$. Dado que 0 y 1 son los únicos cuadrados en módulo 4, m y n deben tener la misma paridad: $m = n + 2l$ para algún $l \in \mathbb{Z}$. Entonces

$$a + b\sqrt{-3} = \frac{m}{2} + \frac{n}{2}\sqrt{-3} = \frac{n + 2l}{2} + n\frac{\sqrt{-3}}{2} = l + n\frac{1 + \sqrt{-3}}{2} = l + n\omega,$$

mostrando que $\mathcal{O} \subset \mathbb{Z} + \mathbb{Z}\omega$. Es fácil comprobar la inclusión inversa. Se tiene que ω satisface la ecuación $\omega^2 - \omega + 1 = 0$, lo que implica, por el criterio 1.3, que $\mathbb{Z} + \mathbb{Z}\omega$ es un anillo. □

Nota. Es posible preguntarse por qué no trabajamos en $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Q}[\sqrt{-3}]$, de manera análoga a los enteros de Gauss y $\mathbb{Q}[i]$. Conviene observar que 4 tiene dos factorizaciones en irreducibles no equivalentes en $\mathbb{Z}[\sqrt{-3}]$:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

$(1 \pm \sqrt{-3})/2$ no está en $\mathbb{Z}[\sqrt{-3}]$, pero es una unidad en $\mathbb{Z}[\omega]$. Trabajando en este anillo ligeramente mas grande, las dos factorizaciones anteriores sí son equivalentes.

$$2 \cdot 2 = (2 \cdot \frac{(1 + \sqrt{-3})}{2}) \cdot (2 \cdot \frac{(1 - \sqrt{-3})}{2}) = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

Del mismo modo que en $\mathbb{Z}[i]$, para estudiar $\mathbb{Z}[\omega]$ vamos a empezar buscando su grupo de unidades. Para ello volveremos a utilizar el concepto de norma definido para los enteros de Gauss, sea $\alpha = a + b\omega$ entonces

$$N\alpha = \alpha\bar{\alpha} = a^2 + ab + b^2$$

Es fácil de probar que las Proposiciones 1.4 y 1.5 se cumplen también para esta norma.

Proposición 1.12. *El grupo de unidades de $\mathbb{Z}[\omega]$ es un grupo cíclico de orden 6 generado por ω:*

$$\mathbb{Z}[\omega]^\times = \{1, \omega, \ldots, \omega^5\}.$$

Demostración. Al igual que en el caso de los enteros de Gauss tenemos que $\epsilon = a + b\omega \in \mathbb{Z}[\omega]^\times$ si y sólo si $N\epsilon = a^2 + ab + b^2 = 1$. Dividiendo por b^2 (en el caso $b = 0$ estaríamos trabajando con números enteros), tenemos que

$$\left(\frac{a}{b}\right)^2 + \frac{a}{b} + 1 = \frac{1}{b^2}.$$

Se tiene que $x^2 + x + 1 \geq 3/4$ para todo $x \in \mathbb{R}$, ya que el vértice de la correspondiente parábola es mayor que $3/4$. Por otra parte, $1/b^2 \leq 1/4$ si $|b| > 1$, forzando a que $b = 0, \pm 1$. Buscamos ahora los posibles valores de a para obtener las correspondientes unidades en $\mathbb{Z}[\omega]$:

$$1 + 0 \cdot \omega = \omega^0, \qquad 0 + 1 \cdot \omega = \omega^1, \qquad -1 + 1 \cdot \omega = \omega^2,$$
$$-1 + 0 \cdot \omega = \omega^3, \qquad 0 - 1 \cdot \omega = \omega^4, \qquad 1 - 1 \cdot \omega = \omega^5$$

□

Podemos probar ya que $\mathbb{Z}[\omega]$ tiene un algoritmo de la división.

Proposición 1.13. *Para cualesquiera $\alpha, \beta \in \mathbb{Z}[\omega]$, $b \neq 0$, existen $\kappa, \lambda \in \mathbb{Z}[\omega]$ tales que $\alpha = \kappa\beta + \lambda$ y $N\lambda < N\beta$.*

Demostración. Observando el retículo que forma $\mathbb{Z}[\omega]$ tenemos que podemos encontrar un elemento $\kappa \in \mathbb{Z}[\omega]$ tal que $N(\alpha/\beta - \kappa) < 1$ (cualquier elemento se encuentra en una traslación del paralelogramo fundamental, y cualquiera de esas traslaciones esta cubierta por dos círculos de radio 1). Poniendo $\lambda = \alpha - \kappa\beta$, tenemos que

$$N\lambda = N(\alpha - \kappa\beta) = N\beta \cdot N\left(\frac{a}{b} - \kappa\right) < N\beta.$$

□

Una vez tenemos el algoritmo de la división, una cadena de proposiciones equivalente a la de la Sección 1.2 nos permite probar el siguiente resultado:

Teorema 1.6 (Factorización única en los Enteros de Eisenstein)**.** *Cualquier elemento de $\mathbb{Z}[\omega]$ que no sea una unidad se puede escribir como un producto de elementos irreducibles. Todas de esas posibles factorizaciones son equivalentes en el sentido de la definición 1.7.*

Teorema 1.7. *Un entero de Eisenstein $\pi \in \mathbb{Z}[\omega]$ es irreducible si y solo si una de las siguientes condiciones se cumple:*

(a) $N\pi = p$ es un primo en $\mathbb{N}$, necesariamente $p \equiv 1 \pmod 3$ o $p = 3$.

(b) $\pi = \epsilon p$, donde $\epsilon \in \mathbb{Z}[\omega]^\times$ y $p \in \mathbb{N}$ es primo con $p \equiv 2 \pmod 3$.

La demostración es análoga a la del teorema 1.5, en este caso el paso determinante es dar respuesta a la pregunta "¿qué primos $p \in \mathbb{Z}$ son de la forma $p = x^2 + xy + y^2$, para ciertos $x, y \in \mathbb{Z}$?".

1.5. El cuerpo $\mathbb{Q}[\sqrt{-5}]$

Los anillos de enteros de $\mathbb{Q}$, $\mathbb{Q}[i]$ y $\mathbb{Q}[\sqrt{-3}]$ tienen todos un algoritmo de la división y por tanto factorización única. Este patrón nos podría hacer ser optimistas y pensar que esta situación se da en todo cuerpo cuadrático. Para ver que esta situación no se cumple en general, vamos a estudiar el cuerpo $\mathbb{Q}[\sqrt{-5}]$.

Proposición 1.14. *El conjunto de los enteros cuadráticos en $\mathbb{Q}[\sqrt{-5}]$ es $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$, y es un anillo.*

Demostración. Es fácil probar que todos los elementos en $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ son enteros cuadráticos. Inversamente, supongamos que $a + b\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$ es un entero cuadrático, y por tanto se satisface que la ecuación $x^2 - 2ax + (a^2 + 5b^2) = 0$ tiene coeficientes en $\mathbb{Z}$. Entonces $a = m/2$ para cierto $m \in \mathbb{Z}$ y $a^2 + 5b^2 = (m^2 + 20b^2)/4$ está en $\mathbb{Z}$. Esto implica que $20b^2 = 20r^2/s^2$ donde r/s es una fracción irreducible. Como m.c.d.$(r, s) = 1$, esto solo ocurre si $s^2 \mid 20$. Así $s = 1$ o $s = 2$.

De cualquier forma, podemos escribir $b = n/2$ para cierto $n \in \mathbb{Z}$, y por tanto $a^2 + 5b^2 = (m^2+5n^2)/4 \in \mathbb{Z}$. Entonces $m^2+n^2 \equiv m^2+5n^2 \equiv 0 \pmod 4$. Dado que los únicos cuadrados

en módulo 4 son 0 y 1, la última congruencia es posible solo cuando tanto m como n son pares. En consecuencia, $a = m/2$ y $b = n/2$ pertenecen a $\mathbb{Z}$, por tanto el entero cuadrático $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$.

Finalmente, $\mathbb{Z}+\mathbb{Z}\sqrt{-5} = \mathbb{Z}[\sqrt{-5}]$ es un anillo por el criterio 1.3, dado que $\sqrt{-5}$ satisface la ecuación mónica $x^2 + 5 = 0$. □

Proposición 1.15. $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$

Demostración. Al igual que en las demostraciones de las proposiciones 1.6 y 1.12, buscamos $\epsilon = a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ tales que $N\epsilon = a^2+5b^2 = \pm 1$. Como $N\epsilon \geq 5$ cuando $b \neq 0$, se tiene que $b = 0$ y $\epsilon = a = \pm 1$. □

Ejemplo 1.1. Veamos que 6 tiene dos factorizaciones en irreducibles no equivalentes en $\mathbb{Z}\sqrt{-5}]$.

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Dado que las únicas unidades de $\mathbb{Z}[\sqrt{-5}]$ son ± 1 es evidente que las dos factorizaciones no son equivalentes. Veamos ahora que $2, 3, (1+\sqrt{-5})$ y $(1-\sqrt{-5})$ son irreducibles en $\mathbb{Z}[\sqrt{-5}]$.

Supongamos que $2 = \alpha\beta$, con $\alpha, \beta \in \mathbb{Z}$ y ninguno de los dos son unidades, es decir, $N\alpha, N\beta > 1$. Dado que $N\alpha \cdot N\beta = N(2) = 4$, tenemos que $N\alpha = N\beta = 2$. Escribiendo $\alpha = a + b\sqrt{-5}$, tenemos que $a^2 + 5b^2 = 2$ y $a^2 \equiv 2 \pmod 5$, lo que es imposible ya que los únicos cuadrados en módulo 5 son 0,1 y 4. En consecuencia 2 es irreducible en $\mathbb{Z}[\sqrt{-5}]$. La prueba para 3 es análoga.

Supongamos ahora que $(1 + \sqrt{-5}) = \alpha\beta$ es una factorización no trivial, tenemos que $N\alpha \cdot N\beta = 6$. Se tiene entonces que $\{N\alpha, N\beta\} = \{2, 3\}$, lo que es imposible por el párrafo anterior.

Ernest Kummer, a mitades del siglo XIX, fue el primero en imaginar una manera de rescatar la factorización única introduciendo el concepto de "números ideales". Vamos a hablar sobre ello como motivación, por tanto aún no los vamos a definir de manera rigurosa. Los trataremos como objetos para los cuales multiplicación y división tienen sentido. En el caso anterior, podemos imaginar que existen números ideales irreducibles P_1, P_2, P_3, P_4 tales que $2 = P_1P_2$, $3 = P_3P_4$, $1 + \sqrt{-5} = P_1P_1$ y $1 - \sqrt{-5} = P_2P_4$.

De esta forma las dos factorizaciones de 6 anteriormente vistas ya no tendrían factores irreducibles y por tanto no tendría por qué ser equivalentes; serían simplemente reordenamientos de una única factorización $6 = P_1P_2P_3P_4$.

Entonces, ¿cómo definimos estos números ideales?. Si van a dar lugar a una división, siendo A un número ideal y $\alpha, \beta, \xi \in \mathbb{Z}[\sqrt{-5}]$, deberán cuplir que

$$A \mid \alpha, A \mid \beta \implies A \mid \alpha + \beta$$

$$A \mid \alpha \implies A \mid \xi\alpha$$

En términos del conjunto $\mathcal{A} = \{\alpha \in \mathbb{Z}[\sqrt{-5}] : A \mid \alpha\}$, las condiciones anteriores simplemente indican que $\mathcal{A}$ es un ideal en el anillo $\mathbb{Z}[\sqrt{-5}]$, ya que es cerrado por sumas internas y por productos externos.

Richard Dedekind, en la segunda mitad del siglo XIX, dio el salto de la idea de Kummer a definir rigurosamente los ideales como los objetos adecuados en los que estudiar la

factorización, probando que para todo ideal en un anillo de enteros distinto de 0, existe una factorización única como producto de ideales primos.

En el siguiente capítulo se definirán rigurosamente los conceptos mencionados en el párrafo anterior.

1.6. El cuerpo $\mathbb{Q}[\sqrt{319}]$

La novedad principal de este ejemplo respecto a los dos anteriores es que $\mathbb{Q}[\sqrt{319}]$ es un cuerpo cudrático real. Los tres cuerpos vistos hasta ahora eran cuerpos cuadráticos imaginarios. Ambos son parecidos en varios sentidos, por ejemplo, determinar el anillo de enteros es parecido en las proposiciones 1.11 y 1.14.

Proposición 1.16. *El conjunto de enteros cuadráticos en* $\mathbb{Q}[\sqrt{319}]$ *es* $\mathbb{Z}+\mathbb{Z}[\sqrt{319}]$*, que es un anillo.*

Dado un $\alpha = a + b\sqrt{319}$, definimos su conjugado en $\mathbb{Q}[\sqrt{319}]$ como $\bar{\alpha} = a - b\sqrt{319}$. La conjugación preserva sumas y multiplicaciones, por tanto, la norma $N\alpha = \alpha\bar{\alpha} = a^2 - 319b^2$, es un homomorfismo multiplicativo. Los cuerpos cuadráticos reales tiene una estructura algo mas compleja que los imaginarios. En $\mathbb{Z}[\sqrt{-5}]$, la norma $N(a+b\sqrt{-5}) = a^2+5b^2$ es siempre positiva y aumenta conforme aumentan $|a|$ o $|b|$. Por tanto la ecuación $a^2 + 5b^2 = n$ tiene soluciones finitas (ninguna si $n < 0$). Por el contrario a^2-319b^2 puede ser positivo o negativo, esta es la raíz de todas las dificultades en el estudio de cuerpos cuadráticos reales.

Por ejemplo, para encontrar las unidades del anillo siguiendo los pasos de los tres ejemplos anteriores, tendríamos que buscar las soluciones enteras de la ecuación de Pell, $x^2 - 319y^2 = \pm 1$. Hay infinitas soluciones, aquella con el valor de x positivo más pequeño es

$$x = 12901780, \qquad y = 722361$$

No podemos esperar encontrar estos números mediante un método de prueba y error. En concreto, hemos elegido $\mathbb{Q}[\sqrt{319}]$ para trabajar porque el tamaño de estas soluciones nos ayuda a ilustrar la necesidad de un algoritmo que permita dar una solución general a la ecuación de Pell, $x^2 - Dy^2 = \pm 1$. Tal algoritmo se obtiene a trabajando con fracciones continuas, por motivos de espacio no vamos a poder introducirlo en este trabajo.

La unidad $\epsilon = 12901780 + 722361\sqrt{319}$, se denomina unidad fundamental de $\mathbb{Z}[\sqrt{319}]$, porque

$$\mathbb{Z}[\sqrt{319}]^\times = \{\pm\epsilon^n : n \in \mathbb{Z}\}.$$

Esa misma teoría de fracciones continuas, permite demostrar que el grupo de unidades de todo cuerpo real cuadrático tiene esta forma, en particular, al contrario de lo que ocurre con los cuerpos cuadráticos imaginarios, los reales tienen infinitas unidades.

Los anillos de enteros de $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{-3}]$ y $\mathbb{Q}[\sqrt{-5}]$ son todos retículos en $\mathbb{C}$. Por el contrario, como se va a comprobar en el ejercicio 1.1, $\mathbb{Z}[\sqrt{319}]$ es un subconjunto denso de la recta real, por tanto no podemos tratar de probar un algoritmo de la divisón teselando el plano con paralelogramos. Más adelante se mostrará como pensar en el anillo de enteros de un cuerpo cuadrático real como un retículo en el plano.

1.7. Ejercicios

Ejercicio 1.1. *Sea η un número irracional, prueba que $\mathbb{Z} + \mathbb{Z}\eta$, y por tanto, $\mathbb{Z}[\sqrt{D}]$, cond D entero libre de cuadrados, es denso en $\mathbb{R}$.*

Sea $(\eta) = \eta - \lfloor \eta \rfloor \in (0,1)$ la parte fraccional de un número irracional $\eta \in \mathbb{R}$, y consideremos el conjunto $\mathcal{K} = \{(k\eta) : k \in \mathbb{Z}\} \in (0,1)$. Dividiendo el intervalo unidad en n subintervalos iguales, y aplicando el Principio del Palomar, tenemos que habrá al menos dos elementos $\alpha, \alpha' \in \mathcal{K}$ en un mismo subintervalo, por tanto $|\alpha - \alpha'| < 1/n$. Ahora bien, para ciertos $k, k' \in \mathbb{Z}$, se tiene que $\alpha - \alpha' = (k\eta) - (k'\eta) = (\lfloor k'\eta \rfloor - \lfloor k\eta \rfloor) + (k - k')\eta$. Por tanto, existen $a, b \in \mathbb{Z}$ tales que $|a + b\eta| < 1/n$ y podemos concluir que $\mathbb{Z} + \mathbb{Z}\eta$ y en particular $\mathbb{Z}[\sqrt{D}]$ son densos en $\mathbb{R}$.

2. Teoría de anillos

En este capítulo daremos un rápido repaso a la teoría de anillos. Definiremos varios conceptos básicos y demostraremos varios resultados que vamos a utilizar a lo largo del trabajo.

2.1. Definiciones básicas

En $\mathbb{Z}$ podemos sumar, restar y multiplicar sin restricciones, pero no siempre podemos dividir; es por ello que las cuestiones sobre divisibilidad tienen interés. Para hacer aritmética en otros sistemas numéricos, abstraemos estas propiedades básicas de $\mathbb{Z}$ para obtener la definición de anillo.

Definición 2.1. Un **anillo** $(R, +, \cdot)$ es un conjunto R con dos operaciones binarias (normalmente denominadas suma y multiplicación) cumpliendo las siguientes propiedades:

(a) $(R, +)$ es un grupo abeliano con elemento identidad 0_R.

(b) La operación $\cdot$ es asociativa, conmutativa y tiene un elemento identidad 1_R.

(c) La multiplicación distribuye respecto a la suma: $\forall a, b, c \in R$, tenemos que $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Un **subanillo** de R es un subconjunto $S \subset R$ que contiene a 1_R y es cerrado por sumas, inversos aditivos y multiplicaciones. Esto convierte a S en un anillo en sí mismo bajo las operaciones heredadas de R. (Salvo confusión, no usaremos los subíndices y escribiremos simplemente 0 y 1 en vez de 0_R y 1_R).

Definición 2.2. Una **unidad** en R es un elemento $a \in R$ para el cual existe un $b \in R$ tal que $ab = 1$.

El elemento b de la definición anterior es único y se conoce como el inverso multiplicativo de b, denotado a^{-1}. El conjunto de todas las unidades $R^\times$ es un grupo multiplicativo.

Definición 2.3. Un anillo F es un **cuerpo** si todo elemento distinto de cero es invertible, es decir, $F^\times = F \backslash 0$.

2.2. Ideales, homomorfismos y cocientes

En el capítulo anterior pudimos intuir la importancia de los ideales en la aritmética de los enteros cuadráticos. Su papel en teoría de anillos es análogo al de los subgrupos normales en teoría de grupos.

Definición 2.4. Sea R un anillo. Un **ideal** $I \subseteq R$ es un subgrupo aditivo que absorbe multiplicaciones: si $a \in I$ y $x \in R$, entonces $ax \in I$.

También nos van a interesar las funciones que respetan la estructura de los anillos.

Definición 2.5. Dados dos anillos R y S, una función $\varphi : R \to S$ es un **homomorfismo de anillos** si cumple las siguientes condiciones para cualquier $a, b \in R$:

(a) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(b) $\varphi(ab) = \varphi(a)\varphi(b)$

(c) $\varphi(1_R) = \varphi(1_S)$

Si φ es inyectiva y suprayectiva, entonces se le llama isomorfismo de anillos. Si existe un isomorfismo entre dos anillos R, S decimos que son isomorfos y lo denotamos como $R \cong S$.

Definición 2.6. El **kernel** de un homomorfismo de anillos $\varphi : R \to S$ es

$$\ker\varphi = \{a \in R : \varphi(a) = 0_S\}$$

Es fácil observar que $\ker\varphi$ es un ideal. Mide lo lejos que está una aplicación de ser inyectiva (lo será si $\ker\varphi = 0_R$).

Dado un anillo R y un ideal I, definimos una relación de equivalencia en R como $a \sim b$ si $a - b \in I$. La clase de equivalencia de a es la clase lateral $a + I = \{a + x : x \in I\}$. El conjunto de todas las clases laterales, se denota $R/I = \{a + I : a \in R\}$.

Proposición 2.1 (Anillo cociente)**.** *Sea I un ideal de un anillo R, entonces las operaciones*

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I)(b + I) = (ab) + I$$

están bien definidas y convierten a R/I en un anillo. La función $\pi : R \to R/I$ definida por $\pi(a) = a + I$ es un homomorfismo de anillos suprayectivo.

Demostración. Tenemos que probar que las operaciones, definidas en términos de representantes de la clase lateral arbitrarios, dependen unicamente de la propia clase lateral. En el caso de la multiplicación, tenemos que probar que si $a+I = a'+I$ y $b+I = b'+I$, entonces $ab+I = a'b'+I$. Sabemos que $a - a', b - b' \in I$. Como I absorbe multiplicaciones, tenemos que $ab-a'b' = a(b-b')+b(a-a') \in I$. Para el caso de la suma basta ver que si $a+I = a'+I$ y $b+I = b'+I$, entonces $a + b - (a' + b') = (a - a') + (b - b') \in I$. □

Teorema 2.1 (Primer teorema de isomorfía)**.** *Sea $\varphi : R \to S$ un homomorfismo de anillos. La asignación $a+ker\varphi \mapsto \varphi(a)$ nos da un isomorfismo de anillos bien definido $\tilde{\varphi} : R/ker\varphi \to \varphi(R)$ que satisface que $\varphi = \pi \circ \tilde{\varphi}$. Decimos que φ induce $\tilde{\varphi}$.*

2.3. Ideales principales

La divisibilidad en un anillo R genérico es tan interesante como lo es en $\mathbb{Z}$. Sean $a, b \in R$, decimos que a divide a b, $a \mid b$, si $b = ac$ para cierto $c \in R$. Si un ideal I de R contiene a a, entonces, por la propiedad de absorción debe contener a todos los elementos divisibles por a. Es decir, $Ra \subseteq I$, donde $Ra = \{ra : r \in R\}$. Es fácil comprobar que Ra es también un ideal, y por tanto, el menor ideal que contiene a a.

Definición 2.7. Un ideal I de R es un **ideal principal** si $I = Ra$ para cierto $a \in R$. A ese a se le conoce como generador de I.

Definición 2.8. Un anillo $\mathcal{D}$ es un **dominio de integridad** si no tiene divisores de 0 : $\forall a, b \in \mathcal{D}$ con $ab = 0$, se tiene que $a = 0$ o $b = 0$.

Los dominios de integridad son precisamente aquellos anillos en los que podemos cancelar elementos: $\forall a, b, c \in \mathcal{D}$ con $a \neq 0, ab = ac$ implica que $b = c$.

Las siguientes propiedades se desprenden directamente de las definiciones de ideal principal y dominio de integridad.

Proposición 2.2. *Sea R un anillo y $a, b \in R$.*

(a) $Ra = R \Leftrightarrow a \in R^\times$

(b) Los tres afirmaciones siguientes son equivalentes: (i) $a \mid b$; (ii) $b \in Ra$; (iii) $Rb \subseteq Ra$.

(c) Sea R un dominio integral. Entonces $Ra = Rb$ si y solo si $a = bu$ para cierto $u \in R^\times$.

Definición 2.9. Un **dominio de ideales principales** (DIP) es un dominio de integridad en el que todo ideal es principal.

Definición 2.10. Sea $\mathcal{D}$ un dominio integral. Una **norma Euclídea** en $\mathcal{D}$ es una función $\nu : \mathcal{D}\backslash 0 \to \mathbb{Z}_{\geq 0}$ con la siguiente propiedad: para cuales quiera $a, b \in \mathcal{D}, b \neq 0$, existen $q, r \in \mathcal{D}$ tales que $a = bq + r$, con $r = 0$ o $\nu(r) < \nu(b)$. Un dominio de integridad $\mathcal{D}$ se llama **dominio Euclídeo** si posee una norma Euclídea. Es importante no confundir la norma Euclídea con la norma definida anteriormente para un cuerpo, $\mathrm{N}\alpha = \alpha\bar{\alpha}$. Ejemplos de normas euclídeas son el valor absoluto en $\mathbb{Z}$ o el grado de un polinomio en $\mathbb{Q}[X]$.

El argumento del Lema 1.1 para $\mathbb{Z}[i]$ se generaliza para probar que un dominio Euclídeo arbitrario es un DIP. De hecho, las demostraciones de factorización única en $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ siguen el mismo esquema:

Algoritmo de la división $\Rightarrow$ Todos los ideales son principales $\Rightarrow$ Algoritmo de Euclides $\Rightarrow$ Lema de Euclides $\Rightarrow$ Factorización única.

Esta cadena prueba la existencia de factorización única tanto en dominios Euclídeos como en DIP (uno empieza en el primer paso, y otro en el segundo). Como hay muchos más DIP que dominios Euclídeos, basaremos nuestro estudio de la aritmética en cuándo un anillo de enteros cuadráticos es un DIP.

2.4. Operaciones con ideales

Vamos a extender varias nociones multiplicativas de elementos de un anillo a ideales, algo parecido a lo que Kummer imaginaba con sus números ideales. La primera definición viene motivada por la Proposición 2.2(b).

Definición 2.11. Sean I y J ideales de un anillo R. Si $J \subseteq I$, decimos que I **divide a** J, escrito $I \mid J$. En el caso concreto en el que $J = Ra$ es principal, escribimos $I \mid a$ que equivale a $I \mid Ra$ y $a \in I$.

Definición 2.12. Dados dos ideales I, J de un anillo R definimos los siguientes conjuntos, cada uno de los cuales es también un ideal:

$$I + J = \{x + y : x \in I, y \in J\}$$

$$I \cap J = \{x \in R : x \in I, x \in J\}$$

$$IJ = \{\sum_{i=1}^{m} x_i y_i : x_i \in I, y_i \in J\}$$

.

Conviene remarcar que:

(a) El ideal $I + J$ es el ideal más pequeño conteniendo tanto a I como a J. En términos de divisibilidad, es el ideal más grande dividiendo a I y a J. Por tanto debemos pensar en $I + J$ como el máximo común divisor de I y J.

(b) En particular, si $I + J = R$, decimos que I y J son ideales coprimos. Esto ocurre si y solo si existen $x \in I$ y $y \in J$ tales que $x + y = 1$.

(c) De manera similar, debemos pensar en $I \cap J$ como el mínimo común múltiplo de I y J.

(d) No podemos definir IJ como el conjunto de los productos xy con $x \in I$ y $y \in J$ ya que no es cerrado por sumas. Por tanto lo hemos definido como el menor ideal que contiene todos los productos xy.

(e) La definición de IJ extiende el producto de elementos de de un anillo a ideales, ya que $(Ra)(Rb) = R(ab)$.

Proposición 2.3 (Teorema Chino del Resto)**.** *Sean I y J dos ideales coprimos de un anillo R. Entonces*

$$R/IJ \cong R/I \times R/J.$$

La estrcutura de anillo en el producto viene dada por sumas y multiplicaciones componente a componente.

Demostración. Para probarlo usaremos el Primer Teorema de Isomorfía, buscando un homomorfismo suprayectivo $\varphi : R \to R/I \times R/J$ con kernel IJ. Sea $\varphi(a) = (a + I, a + J)$, por ser I, J coprimos tenemos que existen $x \in I$, $y \in J$ tales que $x + y = 1$. Sean $a, b \in R$, como $bx + ay = bx + a(1 - x) = b(1 - y) + ay$, tenemos que

$$\varphi(bx + ay) = (a + x(b - a) + I, b + y(a - b) + J) = (a + I, b + J),$$

y por tanto φ es suprayectiva. Obsevemos que $\varphi(a) = (a + I, a + J) = (0 + I, 0 + J)$, el elemento cero de $R/I \times R/J$, si y solo si $a \in I$ y $a \in J$, por tanto, ker$\varphi = I \cap J$. La proposición quedará probada si vemos que para dos ideales coprimos, $I \cap J = IJ$.

La inclusión $\supseteq$ se da siempre. Para $\subseteq$, dado cualquier $a \in I \cap J$ y usando x, y como antes, tenemos que

$$a = a \cdot 1 = a(x + y) = ax + ay \in IJ.$$

□

2.5. Ideales primos y maximales

Antes de generalizar la factorización única para ideales, vamos a decidir cuales son los análogos a los números primos.

Definición 2.13. Un ideal M de un anillo R es **maximal** si $M \neq R$ y R es el único ideal que contiene estrictamente a M.

Definición 2.14. Un ideal P de un anillo R es **primo** si $P \neq R$ y $\forall a, b \in R, ab \in P \Rightarrow a \in P$ o $b \in P$.

Nota. Sea $p \in \mathbb{N}$ primo, $\mathbb{Z}p$ es un ideal primo de $\mathbb{Z}$ ya que si $ab \in \mathbb{Z}p \Rightarrow p \mid ab \Rightarrow p \mid a$ o $p \mid b$. Es fácil ver que $\mathbb{Z}p$ es también maximal.

Proposición 2.4. *Un ideal $P \subset R$ es primo si y solo si R/P es un dominio de integridad.*

Demostración. En el diagrama

$$\begin{array}{ccccc} (a+P)(b+P) = 0+P & \Rightarrow & (a+P = 0+P & \text{o} & b+P = 0+P) \\ \Updownarrow & & \Updownarrow & & \Updownarrow \\ ab \in P & \Rightarrow & (a \in P & \text{o} & b \in P) \end{array}$$

la línea de arriba representa la afirmación de que R/P es un dominio de integridad y la de la abajo la de que P es un ideal primo. □

Proposición 2.5. *Un ideal $M \subset R$ es maximal si y solo si R/M es un cuerpo.*

Demostración. Sea $M \subset R$ un ideal maximal y $a + M \in R/M$ un elemento distinto de 0. Esto implica que $a \notin M \Rightarrow M \subset M + Ra$. Por maximalidad, $M + Ra = R$, luego existen $m \in M, b \in R$ tales que $m + ba = 1$. $(b + M)(a + M) = ba + M = (1 - m) + M = 1 + M$, por tanto $a + M$ tiene inverso multiplicativo. Para la implicación inversa basta con revertir el argumento. □

Corolario 2.1. *Cualquier ideal maximal es ideal primo.*

Veamos ahora una condición suficiente para que un ideal primo sea maximal.

Proposición 2.6. *Sea $\mathcal{D}$ un anillo finito. Entonces $\mathcal{D}$ es un dominio de integridad si y solo si es un cuerpo.*

La demostración es sencilla usando la aplicación $\mu_a(x) = ax$.

Corolario 2.2. *Sea P un ideal primo de un anillo R. Si R/P es finito, entonces P es maximal.*

Definición 2.15. Sea $\mathcal{D}$ un dominio de integridad y $0 \neq p \in \mathcal{D} \backslash \mathcal{D}^\times$.

(a) p es **irreducible** si, $\forall a, b \in R, p = ab \Rightarrow a \in \mathcal{D}^\times$ o $b \in \mathcal{D}^\times$.

(b) p es un elemento **primo** si, $\forall a, b \in R, p \mid ab \Rightarrow p \mid a$ o $p \mid b$.

Proposición 2.7. *Sea $\mathcal{D}$ un dominio de integridad.*

(a) Un elemento $p \in \mathcal{D}$ es primo si y solo si $\mathcal{D}p$ es un ideal primo.

(b) Cualquier elemento primo de $\mathcal{D}$ es irreducible (el recíproco no siempre es cierto).

2.6. Ejercicios

Ejercicio 2.1. *Sea P un ideal de un anillo R. Demuestra que P es un ideal primo si y solo si la siguiente afirmación análoga al Lema de Euclides se cumple para cuales quiera dos ideales I, J de R:*

$$P \mid IJ \Leftrightarrow P \mid I \vee P \mid J.$$

Veamos que si P es primo, se cumple la afirmación. Supongamos que $P \mid IJ$ pero $P \nmid I$ y $P \nmid J$. Entonces existen $a \in I$, $b \in J$ tales que $a \notin P$ y $b \notin P$. Por ser P primo, tenemos que $ab \notin P$, pero $ab \in IJ$, luego hemos llegado a una contradicción. Inversamente, si $P \mid I$, dado que los ideales absorben multiplicaciones, y por tanto $IJ \subseteq I$, tenemos que $P \mid IJ$.

Ahora veamos que si se cumple la afirmación, P es primo. Supongamos que P no es primo, por tanto, existe $ab \in P$ tal que $a \notin P$ y $b \notin P$. Dado que $ab \in P$, tenemos que $P \mid Rab = RaRb \Leftrightarrow P \mid Ra \vee P \mid Rb \Leftrightarrow a \in P \vee b \in P$, lo que es una contradicción. Por tanto P es primo.

Ejercicio 2.2. *Prueba que $D = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ no es un Dominio Euclídeo.*

Trabajaremos por reducción al absurdo, suponiendo que existe un norma Euclídea fuerte ν en D. Una norma Euclídea fuerte tiene la condición añadida $\nu(a) \leq \nu(ab)$ $\forall a, b \in D\backslash 0$. En todo Dominio Euclídeo, la fórmula

$$\nu'(a) = \min\{\nu(ax) : x \in D\backslash 0\}$$

Define una norma Euclídea fuerte, luego podemos trabajar con ella sin perdida de generalidad.

(a): Cálculemos $D^\times$. $\alpha \in D^\times$ si y solo si $N\alpha = 1$. $\alpha = a + b(\frac{1+\sqrt{-19}}{2})$, $N\alpha = \alpha\bar{\alpha} = a^2 + b^2/4 + ab + 19b^2/4 = a^2 + ab + 5b^2$. Por tanto, $N\alpha \geq 5$ si $b \neq 0$, luego $b = 0$ y $\alpha = \pm 1$.

(b): Veamos que 2 y 3 son irreducibles. Si 2 no fuera irreducible, entonces $2 = \alpha\beta$ con $N\alpha$,$N\beta \neq 1$. Tomando normas, $4 = N\alpha N\beta$, luego $N\alpha$,$N\beta = \pm 2$. Imposible, ya que la ecuación $a^2 + ab + 5b^2 = \pm 2$ obliga a $b = 0$ y $a^2 = \pm 2$ no tiene soluciones enteras. Análogamente tenemos que 3 es irreducible, en este caso $N\alpha$,$N\beta = \pm 3$ y procederíamos de la misma forma.

(c) Sea $m = min\{\nu(a) : a \in D\backslash 0\}$, y $M = \{u \in D\backslash 0 : \nu(u) = m\}$ el conjunto de elementos de norma Euclídea mínima. Tenemos que $D^\times \subseteq M$, ya que $\nu(1) \leq \nu(1 \cdot a) = \nu(a), \forall a \in D\backslash 0$, luego $1 \in M$ y $m = \nu(1)$. En consecuencia, si $\alpha\beta = 1$, $\nu(\alpha) \leq \nu(\alpha\beta) = \nu(1)$, luego $\alpha \in M$. Pero también se cumple que $M \subseteq D^\times$; sea $\alpha \in M$, entonces $1 = \alpha q + r$ con $r = 0$ o $\nu(r) < \nu(\alpha)$, luego $r = 0$ y $1 = \alpha q$. Así, $M = D^\times$.

Ahora, sea $a \in D$ un elemento con la norma Euclídea más pequeña después de m. Es decir, $\forall \alpha \in D$, se tiene que $\alpha = aq + r$ con $r = 0$ o $\nu(r) < \nu(a)$, así que $r = 0$ o $r \in D^\times$. Hemos visto que $D^\times = \{\pm 1\}$, luego el cociente D/Da tendrá a lo sumo 3 clases.

(d): Vamos a ver que $a \mid 2$ o $a \mid 3$ y llegaremos a una contradicción con (b). D/Da tendrá dos clases si y solo si $2 \in Da$, es decir, $a \mid 2$. Supongamos que $a \nmid 2$, entonces en D/Da tenemos tres clases y $2 \notin Da$, además $\bar{1} \neq \bar{2}$, luego tenemos que las clases son $\bar{0}, \bar{1}, \bar{2}$. Por tanto, $\bar{3}$ es una de esas tres clases, pero $\bar{3} \neq \bar{1}$, ya que $2 \notin Da$, y $\bar{3} \neq \bar{2}$ ya que $1 \notin Da$ (ya que a no es invertible). Luego $\bar{0} = \bar{3}$ y $a \mid 3$ y hemos llegado a una contradicción.

En el Ejemplo 5.3 veremos que a pesar de no ser un Dominio Euclídeo, $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ sí es un DIP.

3. Retículos

En este capítulo estudiaremos unas nociones básicas acerca de la teoría de retículos. Los retículos serán una herramienta fundamental durante el trabajo, ya que nos permiten dibujar en el plano los anillos de enteros, además de ampliar la reducción gaussiana a matrices con entradas en $\mathbb{Z}$.

3.1. Estructura de grupo de los retículos

La mayoría de los anillos e ideales que hemos visto en el primer capítulo son retículos. En cierto modo, podemos pensar en ellos como "espacios vectoriales con coeficientes en $\mathbb{Z}$", y trabajar con ellos con las herramientas del álgebra lineal. En las demostraciones del algoritmo de la división en $\mathbb{Z}[i]$ y $\mathbb{Z}[\omega]$ nos basamos en buena medida en la geometría de los retículos como subconjuntos de un plano, $\mathbb{R}^2$ o $\mathbb{C}$.

Definición 3.1. Sea V un plano, un **retículo** $\Lambda \subset V$ es un subgrupo aditivo de V de la forma $\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2 = \{av_1 + bv_2 : a, b \in \mathbb{Z}\}$, donde los vectores $v_1, v_2 \in V$ son linealmente independientes sobre $\mathbb{R}$. A cada uno de esos pares $\{v_1, v_2\}$ se les denomina **base** de Λ.

Nota. Denotaremos Λ_0 (resp. V_0) al grupo (resp. $\mathbb{R}$-espacio vectorial) de 2×1 vectores columna con entradas en $\mathbb{Z}$ (resp. $\mathbb{R}$). Tomamos $\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\}$ como base para ambos. Utilizaremos Λ_0 como nuestro retículo estándar. Para cualquier retículo $\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2$ dentro de un plano V, la asignación

$$\begin{bmatrix}1\\0\end{bmatrix} \mapsto v_1, \qquad \begin{bmatrix}0\\1\end{bmatrix} \mapsto v_2$$

define un isomorfismo $\mathbb{R}$-lineal $V_0 \xrightarrow{\sim}$ V cuya restricción a Λ_0 es un isomorfismo de grupos abelianos $\Lambda_0 \to \Lambda$

Definición 3.2. Sea $\Lambda = \mathbb{Z}v_1 + \mathbb{Z}v_2 \subset V$ un retículo. El **paralelogramo fundamental** de Λ respecto a la base $\{v_1, v_2\}$ es el conjunto

$$\prod_{\{v_1,v_2\}} = \{t_1v_1 + t_2v_2 : t_1, t_2 \in [0, 1)\} \subset V$$

La independencia lineal de v_1 y v_2 implica que el plano queda teselado por las traslaciones $v + \prod_{\{v_1,v_2\}}$, con v recorriendo Λ.

Proposición 3.1. *Para que cualquier $w \in V$ existe un único par $a, b \in \mathbb{Z}$ tal que $w - (av_1 + av_2)$ está en el paralelogramo fundamental $\prod_{\{v_1,v_2\}}$.*

Como hemos visto en la Proposición anterior, el estudio de la estructura de grupo de cualquier retículo se reduce al estudio del retículo estándar Λ_0.

Teorema 3.1. *Si $A \subseteq \Lambda_0$ es un subgrupo, entonces A es uno de los siguientes:*

(a) 0;

(b) $\mathbb{Z}t$, para cierto $t \in \Lambda_0$;

(c) $\mathbb{Z}t_1 + \mathbb{Z}t_2$*, para dos vectores linealmente independientes* $t_1, t_2 \in \Lambda_0$*. Un subgrupo de esta forma se denomina subretículo.*

Lema 3.1. *Si* $t_1, t_2 \in \Lambda_0$ *y* $t_2 = \alpha t_1, \alpha \in \mathbb{R}$*, entonces* t_1 *y* t_2 *son linealmente dependientes sobre* $\mathbb{Z}$*.*

Demostración. Sea $t_1 = \begin{bmatrix} r_1 \\ s_1 \end{bmatrix}$ y $t_2 = \begin{bmatrix} r_2 \\ s_2 \end{bmatrix} = \alpha \begin{bmatrix} r_1 \\ s_1 \end{bmatrix}$. Podemos asumir también que $r_1 \neq 0$, luego $\alpha = r_2/r_1$, y

$$r_2 t_1 - r_1 t_2 = r_2 t_1 - r_1 \left(\frac{r_2}{r_1}\right) t_1 = 0$$

□

Demostración Teorema 3.1. Supongamos que $A \neq 0$. Definimos la función distancia al cuadrado $\lambda : \Lambda_0 \to \mathbb{Z}_{\geq 0}$ como $\lambda(ab) = a^2 + b^2$. Elegimos un $t_1 \in A$ distinto de 0 para el cual $\lambda(t_1)$ es mínimo en $A \backslash 0$. Si $A = \mathbb{Z}t_1$, estamos en el caso (b).

Supongamos que $A \neq \mathbb{Z}t_1$. Sea t_2 uno de los elementos de medida mínima en $A \backslash \mathbb{Z}t_1$. Se tiene que t_1 y t_2 son linealmente independientes sobre $\mathbb{Z}$ (y por tanto sobre $\mathbb{R}$). Si no lo fueran, existirían $a, b \in \mathbb{Z}$ tales que $at_1 = bt_2$. El algoritmo de la división produce $q, r \in \mathbb{Z}$ tales que $a = qb + r$ y $0 \leq r < |b|$. Sea $t' = (r/b)t_1 = (r/a)t_2 = t_2 - qt_1$, que está en A, dado que A es un grupo. Tenemos que $\lambda(t') = (r/b)^2 \lambda(t_1) < \lambda(t_1)$, lo que contradice la elección de t_1 como el elemento más corto de A, salvo que $t' = t_2 - qt_1 = 0$, pero esto contradice que $t_2 \notin \mathbb{Z}t_1$.

Supongamos que existe $x \in A \backslash (\mathbb{Z}t_1 + \mathbb{Z}t_2)$. Después de trasladarlo por una combinación lineal de t_1 y t_2 podemos asumir que x está en el paralelogramo fundamental $\prod_{\{t_1, t_2\}}$. Como $\lambda(x) \geq \lambda(t_2)$ por como hemos elegido t_2, x está sobre o fuera de la circunferencia de radio $\sqrt{\lambda(t_2)}$ centrado en 0. Por tanto, como x está en el paralelogramo fundamental, está a una distancia menor que $\sqrt{\lambda(t_1)}$ de $t_1 + t_2$. Esto implica que $\lambda(x - t_1 - t_2) < \lambda(t_1)$, contradiciendo que $x - t_1 - t_2 \in A \backslash 0$. □

3.2. Álgebra lineal sobre $\mathbb{Z}$

Las matrices con las que vamos a trabajar siempre van a tener sus entradas en $\mathbb{Z}$, por tanto las únicas operaciones de filas y columnas que vamos a permitir son aquellas que no introducen denominadores.

Para cualquier anillo R, denotamos por $M_{k \times l}(R)$ al grupo aditivo de matrices $k \times l$ con entradas en R. Cuando $k = l$, $M_{k \times k}(R)$ es un anillo no conmutativo bajo la multiplicación de matrices. Su grupo de unidades, denotado $GL_k(R)$, son las matrices invertibles, es decir, aquellas con determinante en $R^\times$.

Los resultados que se van a exponer a continuación son fáciles de demostrar. Se puede encontrar su demostración en el capítulo

Proposición 3.2. *Sea* $\gamma \in M_{2 \times 2}(\mathbb{R})$*. Entonces* $\gamma \in M_{2 \times 2}(\mathbb{Z})$ *si y solo si* $\gamma \Lambda_0 \subseteq \Lambda_0$*.*

Corolario 3.1. *Sea* $\gamma \in M_{2 \times 2}(\mathbb{R})$*. Entonces* $\gamma \Lambda_0 = \Lambda_0$ *si y solo si*

$$\gamma \in GL_2(\mathbb{Z}) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = \pm 1 \}.$$

Corolario 3.2. *Un subgrupo $\Lambda \subseteq \Lambda_0$ es un subretículo si y solo si existe $\gamma \in M_{2\times 2}(\mathbb{Z})$ tal que $\Lambda = \gamma\Lambda_0$ y $det\gamma \neq 0$.*

Definición 3.3. Una matriz $k \times l$ está en **forma reducida por columnas** si tiene una matriz triangular superior de tamaño máximo, $\min(k,l)\times\min(k,l)$, en su esquina superior derecha, y ceros en el resto.

Teorema 3.2 (Reducción integral por columnas)**.** *Cualquier matriz con entradas en $\mathbb{Z}$ se puede poner en forma reducida por columnas mediante una serie de operaciones columna enteras.*

Más adelante veremos varios ejemplos de reducción por columnas para hacer cálculos con ideales.

Definición 3.4. Sea $A \in M_{k\times l}(\mathbb{Z})$. Definimos col$A$, el **grupo columna** de A, como el grupo aditivo de todas las combinaciones $\mathbb{Z}$-lineales de columnas de A.

Estamos interesados en col$A$ porque es invariante bajo operaciones columna.

Proposición 3.3. *Sea A' una matriz obtenida de otra matriz A mediante una series de operaciones columna enteras. Entonces colA' =col$A$.*

Demostración. Todas las operaciones columna se basan en permutaciones y combinaciones $\mathbb{Z}$-lineales de columnas. El grupo col$A$ es cerrado por ambas, por tanto col$A' \subseteq$ col$A$. La inclusión inversa se cumple porque toda operación columna se puede deshacer mediante otra del mismo tipo. □

3.3. Cálculos con ideales

La reducción por columnas es una herramienta esencial a la hora de hacer cuentas con ideales, vamos a verlo en varios ejemplos.

Ejemplo 3.1. Calculemos el producto de los ideales $I = \mathbb{Z}\cdot 3 + \mathbb{Z}(1-\sqrt{-5})$ y $J = \mathbb{Z}\cdot 7 + \mathbb{Z}(3+\sqrt{-5})$. El ideal IJ está formado por las combinaciones $\mathbb{Z}$-lineales de $3\cdot 7, 3(3+\sqrt{-5}), 7(1-\sqrt{-5})$ y $(3+\sqrt{-5})(1-\sqrt{-5})$. El retículo Λ_{IJ} es por tanto el grupo columna de la siguiente matriz, y no cambia cuando se le aplica reducción por columnas:

$$A = \begin{bmatrix} 21 & 9 & 7 & 8 \\ 0 & 3 & -7 & -2 \end{bmatrix} \xrightarrow[C_2+C_4]{C_3-3C_4} \begin{bmatrix} 21 & 17 & -17 & 8 \\ 0 & 1 & -1 & -2 \end{bmatrix} \xrightarrow{C_2 \circlearrowleft C_4} \begin{bmatrix} 21 & 8 & -17 & 17 \\ 0 & -2 & -1 & 1 \end{bmatrix} \xrightarrow[C_2+2C_4]{C_3+C_4}$$

$$\begin{bmatrix} 21 & 42 & 0 & 17 \\ 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{C_2-2C_1} \begin{bmatrix} 21 & 0 & 0 & 17 \\ 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[C_1 \circlearrowleft C_3]{C_4-C_1} \begin{bmatrix} 0 & 0 & 21 & -4 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Trasladando el resultado de vectores en Λ_0 a elementos de $\mathbb{Z}[\sqrt{-5}]$, tenemos que $IJ = \mathbb{Z}\cdot 21 + \mathbb{Z}(-4+\sqrt{-5})$.

Ejemplo 3.2. Calculemos $I+J$ para los ideales $I = \mathbb{Z}\cdot 3+\mathbb{Z}(1+\sqrt{-5})$ y $J = \mathbb{Z}\cdot 3+\mathbb{Z}(1-\sqrt{-5})$. Por definición, $I+J$ es el menor ideal que contiene a I y a J. Obtenemos sus generadores

colocando juntos los generadores de I y J: $3, 1+\sqrt{-5}, 3, 1-\sqrt{-5}$, y buscamos una base del grupo columna de la matriz:

$$\begin{bmatrix} 3 & 1 & 3 & 1 \\ 0 & 1 & 0 & -1 \end{bmatrix} \xrightarrow[C_1-C_3]{C_2+C_4} \begin{bmatrix} 0 & 2 & 3 & 1 \\ 0 & 0 & 0 & -1 \end{bmatrix} \xrightarrow[C_3-C_2]{-C_4} \begin{bmatrix} 0 & 2 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[C_2-2C_3]{C_4+C_3} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Por tanto $I + J = \mathbb{Z} + \mathbb{Z}\sqrt{-5} = \mathbb{Z}[\sqrt{-5}]$, es decir, I y J son ideales coprimos.

Ejemplo 3.3. Calculemos $I \cap J$ para $I = \mathbb{Z} \cdot 21 + \mathbb{Z}(4+\sqrt{-5})$ y $J = \mathbb{Z} \cdot 18 + \mathbb{Z}(4+2\sqrt{-5})$. Si $\alpha \in I \cap J$, existen $a, b, c, d \in \mathbb{Z}$ con $\alpha = a \cdot 21 + b(4+\sqrt{-5}) = c \cdot 18 + d(4+2\sqrt{-5})$. Comparando coeficientes, obtenemos el siguiente sistema:

$$21a + 4b - 18c - 4d = 0$$

$$b - 2d = 0.$$

La solución, con c y d como variables libres, es

$$a = \frac{2(9c-2d)}{21}, b = 2d,$$

donde a, b, c, d deben estar en $\mathbb{Z}$. Esto impone la siguiente condición, $2d \equiv 9c \pmod{21}$, que se cumple si $d = 15c + 21k$ para ciertos $c, k \in \mathbb{Z}$. Por tanto, podemos escribir α como:

$$\alpha = c \cdot 18 + d(4+2\sqrt{-5}) = c \cdot (78 + 30\sqrt{-5}) + k(84 + 42\sqrt{-5}),$$

luego $I \cap J = \mathbb{Z}(78+30\sqrt{-5}) + \mathbb{Z}(84+42\sqrt{-5})$. Para simplificar aplicamos reducción por columnas:

$$\begin{bmatrix} 78 & 84 \\ 30 & 42 \end{bmatrix} \to \begin{bmatrix} 78 & 6 \\ 30 & 12 \end{bmatrix} \to \begin{bmatrix} 66 & 6 \\ 6 & 12 \end{bmatrix} \to \begin{bmatrix} 66 & -126 \\ 6 & 0 \end{bmatrix} \to \begin{bmatrix} 126 & 66 \\ 0 & 6 \end{bmatrix}$$

Finalmente, $I \cap J = \mathbb{Z} \cdot 126 + \mathbb{Z}(66+6\sqrt{-5})$.

3.4. Cocientes de retículos

Hemos trabajado con operaciones integrales por columnas, pero, ¿qué ocurre con las operaciones por filas?. Sean $\alpha, \gamma \in M_{k\times k}(\mathbb{Z})$, con α invertible. El producto $\gamma\alpha$ se puede calcular como una serie de operaciones integrales por columnas, del mismo modo, $\alpha\gamma$ se puede calcular con una serie de operaciones integrales por filas. Las operaciones por filas son menos importantes debido a la siguiente asimetría:

Cada $\gamma \in M_{k\times k}(\mathbb{Z})$, con $\det\gamma \neq 0$ determina un subretículo $\Lambda = \gamma\Lambda_0$. Entonces $(\gamma\alpha)\Lambda_0 = \gamma\Lambda_0 = \Lambda$, pero $(\alpha\gamma)\Lambda_0 = \alpha\Lambda$. Multiplicar γ por α por la derecha no cambia Λ, pero multiplicando por la izquierda cambia Λ por un retículo isomorfo, pero en general distinto.

Teorema 3.3 (Reducción integral por filas y columnas)**.** *Sea $X \in M_{k\times l}(\mathbb{Z})$, y $n = min(k, l)$. Existe una secuencia de operaciones fila y columna que convierte a X en una matriz en forma normal: en la esquina inferior derecha tiene una submatriz diagonal $n \times n$*

$$\begin{bmatrix} d_n & 0 & \cdots & 0 \\ 0 & d_{n-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & d_1 \end{bmatrix}$$

con $d_1 \mid d_2 \mid \cdots \mid d_n$.

La prueba de este teorema se puede obtener como corolario de la teoría de módulos estudiada en la asignatura optativa *Álgebra y aplicaciones*. Se trata de una consecuencia del Teorama 5.2 del capítulo IV de módulos del libro *Algebra*, de Larry C. Groove [5].

Ejemplo 3.4. Sea $\Lambda = \gamma\Lambda_0$, con $\gamma = \begin{bmatrix} -2 & 6 \\ 6 & 14 \end{bmatrix}$, para calcular Λ_0/Λ, aplicamos la reducción integral por filas y columnas:

$$\begin{bmatrix} -2 & 6 \\ 6 & 14 \end{bmatrix} \xrightarrow[F_2+3F_1]{-C_1} \begin{bmatrix} 2 & 6 \\ 0 & 32 \end{bmatrix} \xrightarrow{C_2-3C_1} \begin{bmatrix} 2 & 0 \\ 0 & 32 \end{bmatrix} \xrightarrow[C_1 \circlearrowright C_2]{F_1 \circlearrowright F_2} \begin{bmatrix} 32 & 0 \\ 0 & 2 \end{bmatrix}$$

El último cambio de filas y columnas ha sido necesario para obtener la condición $d_1 \mid d_2$. Ahora ya podemos encontrar el cociente:

$$\Lambda_0/\Lambda \cong (\mathbb{Z}\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \mathbb{Z}\begin{bmatrix} 0 \\ 1 \end{bmatrix})/(\mathbb{Z}\begin{bmatrix} 32 \\ 0 \end{bmatrix} + \mathbb{Z}\begin{bmatrix} 0 \\ 2 \end{bmatrix}) \cong \mathbb{Z}/32\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Proposición 3.4. *Sea $\Lambda = \gamma\Lambda_0$ para cierto $\gamma \in M_{2\times 2}$ con $det\ \gamma \neq 0$. El cociente Λ_0/Λ es finito y $|\Lambda_0/\Lambda| = |det\ \gamma|$.*

Demostración. Sean $\alpha, \beta \in \mathrm{GL}_2(\mathbb{Z})$ las matrices correspondientes a las secuencias de operaciones fila y columna, respectivamente, que diagonalizan γ como en el teorema anterior:

$$\alpha\gamma\beta = \begin{bmatrix} d_2 & 0 \\ 0 & d_1 \end{bmatrix} = \gamma', d_1 \mid d_2.$$

Entonces $\Lambda_0/\Lambda = \Lambda_0/\gamma\Lambda_0 = \Lambda_0/(\alpha^{-1}\gamma'\beta^{-1})\Lambda_0 = \Lambda_0/(\alpha^{-1}\gamma'\Lambda_0) \cong \Lambda_0/\gamma'\Lambda_0 \cong \mathbb{Z}/d_2\mathbb{Z} \times \mathbb{Z}/d_1\mathbb{Z}$.

Claramente $|\Lambda_0/\Lambda| = d_1d_2$. Por otra parte, $\det\gamma = (\det\alpha^{-1})\det\gamma'(\det\beta^{-1}) = (\pm1)(d_1d_2)(\pm1)$, por tanto $|\Lambda_0/\Lambda| = |\det\gamma|$. □

4. Aritmética en $\mathbb{Q}[\sqrt{D}]$

El siguiente capítulo es el más importante del trabajo. En él desarrollaremos la teoría de números algebraica para un cuerpo cuadrático genérico. El capítulo culmina con la demostración de uno de los dos resultados principales del trabajo, la factorización única de ideales.

4.1. Cuerpos cuadráticos

En el primer capítulo, mediante los ejemplos de $\mathbb{Q}[i], \mathbb{Q}[\sqrt{-3}], \mathbb{Q}[\sqrt{-5}]$ y $\mathbb{Q}[\sqrt{319}]$ nos pudimos hacer una idea de las particularidades que tiene estudiar la aritmética de cuerpos más grandes que $\mathbb{Q}$: factorización no única, importancia de los ideales, grupos infinitos de unidades... En este capítulo vamos a trabajar en esas particularidades a través de un cuerpo cuadrático genérico.

Definición 4.1. Un **cuerpo cuadrático** es un cuerpo de la forma

$$\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\},$$

donde $D \in \mathbb{Z}$ no es un cuadrado perfecto. El cuerpo se dice imaginario si $D < 0$, y real si $D > 0$.

Salvo que se especifique lo contrario, toda la teoría que vamos a desarrollar vale tanto para cuerpos reales como para imaginarios. Decimos que D es libre de cuadrados si no es divisible por ningún cuadrado perfecto salvo el 1; es decir, es un producto de primos distintos. Cuando trabajamos en $\mathbb{Q}[\sqrt{D}]$, es útil asumir que D es libre de cuadrados, lo podemos hacer sin pérdida de generalidad, ya que si $D' = n^2 D$, entonces $a + b\sqrt{D'} = a + bn\sqrt{D}$, luego $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$.

Definición 4.2. Sea $\alpha \in \mathbb{Q}[\sqrt{D}]$. El **conjugado** de $\alpha = a + b\sqrt{D}$ es $\bar{\alpha} = a - b\sqrt{D}$. Definimos la **traza** y la **norma** de α como

$$\text{Tr } \alpha = \alpha + \bar{\alpha}, \qquad \text{N}\alpha = \alpha\bar{\alpha}.$$

Sea $\alpha \in \mathbb{Q}[\sqrt{D}] \backslash \mathbb{Q}$, la traza y la norma de α aparecen de manera natural cuando buscamos los polinomios $p(x) \in \mathbb{Q}[x]$ tales que $p(\alpha) = 0$ ya que entonces $p(\bar{\alpha}) = 0$, luego $p(x)$ debe ser divisible por

$$(x - \alpha)(x - \bar{\alpha}) = x^2 - (Tr\alpha) + N\alpha.$$

Proposición 4.1. *Sea $\alpha \in \mathbb{Q}[\sqrt{D}]$:*

(a) Sean $a, b \in \mathbb{Q}$, tenemos que

$$Tr(a + b\alpha) = 2a + (Tr\ \alpha)b$$
$$N(a + b\alpha) = a^2 + (Tr\alpha)ab + (N\alpha)b^2.$$

(b) Tr α y N α son racionales. Las funciones Tr: $\mathbb{Q}[\sqrt{D}] \to \mathbb{Q}$ y N: $\mathbb{Q}[\sqrt{D}]^\times \to \mathbb{Q}^\times$ son homomorfismos de grupos aditivos y multiplicativos respectivamente.

(c) *α es raíz de $x^2-(Tr\ \alpha)x+N\alpha$, siendo este el único polinomio cuadrático, mónico y con coeficientes racionales que lo cumple (salvo que $\alpha \in \mathbb{R}$).*

(d) *$\alpha \in \mathbb{Q}$ si y solo si $\alpha = \bar{\alpha}$.*

(e) *La función $\alpha \to \bar{\alpha}$ es el único homomorfismo de anillos distinto de la identidad en $\mathbb{Q}[\sqrt{D}] \to \mathbb{Q}[\sqrt{D}]$.*

Demostración. Las cuatro primeras propiedades se obtienen directamente de las definiciones. Probemos la propiedad (e):

Sea $\varphi : \mathbb{Q}[\sqrt{D}] \to \mathbb{Q}[\sqrt{D}]$ un homomorfismo de anillos. Tenemos que $\varphi(1) = 1 \Rightarrow \varphi(-1) = -1$ de donde se tiene que $\varphi(z) = z, \forall z \in \mathbb{Z}$. Ahora $1 = \varphi((1/z)z) \Rightarrow \varphi(1/z) = 1/z$ por tanto, $\forall q \in \mathbb{Q}, \varphi(q) = q$. Por último, $\varphi(\sqrt{D})\varphi(\sqrt{D}) = D \Rightarrow \varphi(\sqrt{D}) = \pm\sqrt{D}$, es decir, φ es el homomorfismo identidad o $\varphi(\alpha) = \bar{\alpha}$. □

4.2. El anillo de enteros

Vamos a ampliar la definición dada en el primer capítulo a un cuerpo cuadrático genérico.

Definición 4.3. El **anillo de enteros** de $\mathbb{Q}[\sqrt{D}]$ es el conjunto

$$\begin{aligned}\mathcal{O} &= \{\alpha \in \mathbb{Q}[\sqrt{D}] : \alpha^2 - t\alpha + n = 0 \text{ para ciertos } t, n \in \mathbb{Z}\} \\ &= \{\alpha \in \mathbb{Q}[\sqrt{D}] : \text{Tr } \alpha, \text{ N } \alpha \in \mathbb{Z}\}.\end{aligned}$$

La segunda igualdad es la proposición 4.1(c). Veamos ahora que $\mathcal{O}$ es en efecto un anillo.

Teorema 4.1. *Sea $D \in \mathbb{Z}$ libre de cuadrados, el conjunto de enteros en $\mathbb{Q}[\sqrt{D}]$ es un anillo dado por $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\delta_0 = \mathbb{Z}[\delta_0]$, donde*

$$\delta_0 = \begin{cases} \sqrt{D} & si\ \ D \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & si\ \ D \equiv 1 \pmod 4 \end{cases}$$

Demostración. En ambos casos $\delta_0 \in \mathcal{O}$, ya que es raíz de una ecuación cuadrática y mónica, con coeficientes en $\mathbb{Z}$, en el primer caso, $x^2 - D$, en el segundo $x^2 - x + (1 - D)/4$. La segunda ecuación tiene coeficientes en $\mathbb{Z}$ precisamente cuando $D \equiv 1 \pmod 4$. Es evidente que $\mathbb{Z} + \mathbb{Z}\delta_0 \subseteq \mathcal{O}$, nos centraremos en probar la inclusión inversa.

Tomemos un $\alpha = a + b\sqrt{D} \in \mathcal{O}$. Por la definición 4.3 esto significa que Tr $\alpha = 2a$ y N $\alpha = a^2 - b^2D$ están ambos en $\mathbb{Z}$. Escribimos $a = r/2, b = m/n$ para ciertos $r, m, n \in \mathbb{Z}$ con m.c.d.$(m, n) = 1$. Entonces $4m^2D = n^2(r^2 - 4\text{N}\alpha)$, luego $n^2 \mid 4m^2D$, en concreto $n^2 \mid 4D$ ya que m.c.d.$(m, n) = 1$. Si existiera un p factor primo impar de n, tendríamos que $p^2 \mid D$, contradiciendo que D es libre de cuadrados, luego n es una potencia de 2. Como $4 \nmid D$, $n^2 \mid 4D$ implica que $n^2 \mid 8$, luego $n = 1$ o 2. En cualquier caso, $b = s/2$, para cierto $s \in \mathbb{Z}$.

Dado que $a^2 - b^2D \in \mathbb{Z}$, tenemos que $r^2 \equiv s^2D \pmod 4$. Consideramos dos casos, teniendo en cuenta que los únicos cuadrados en modulo 4 son 0 y 1:

(a) Si $D \not\equiv 1 \pmod 4$, entonces el par (r, s) satisface $r^2 \equiv s^2 \equiv 0 \pmod 4$. Esto implica que r y s son enteros pares, luego a y b están en $\mathbb{Z}$ y $\mathcal{O} \subseteq \mathbb{Z} + \mathbb{Z}\sqrt{D}$.

(b) Si $D \equiv 1 \pmod 4$, entonces $r^2 \equiv s^2 D \equiv s^2 \pmod 4$, lo que implica que $r \equiv s \pmod 2$. Escribiendo $r = s + 2k$, para $k \in \mathbb{Z}$ observamos que

$$\alpha = a + b\sqrt{D} = \frac{r + s\sqrt{D}}{2} = \frac{s + 2k + s\sqrt{D}}{2} = k + s\frac{1 + \sqrt{D}}{2}.$$

Luego $\mathcal{O} \subseteq \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{D}}{2}$.

□

Por la proposción 4.1 (c), cualquier $\alpha \in \mathcal{O}\backslash\mathbb{Z}$ es raíz de un único polinomio mónico cuadrático con coeficientes en $\mathbb{Z}$, lo que sugiere que un invariante de ese polinomio será también un invariante de α.

Definición 4.4. El **discriminante** de $\alpha \in \mathcal{O}$ es $\operatorname{disc} \alpha = (\operatorname{Tr}\alpha)^2 - 4\operatorname{N}\alpha$.

Las siguientes propiedades se obtienen directamente de la definición de discriminante.

Proposición 4.2. *Sea $\alpha \in \mathcal{O}$ y $\beta \in \mathbb{Z}[\alpha] \subseteq \mathcal{O}$. Entonces disc $\beta = c^2 \cdot$ disc α, para cierto $c \in \mathbb{N}$.*

Corolario 4.1. *Sea $\alpha, \beta \in \mathcal{O}$.*

(a) Si $\mathbb{Z}[\beta] \subseteq \mathbb{Z}[\alpha]$, entonces disc $\alpha \mid$ disc β.

(b) Si $\mathbb{Z}[\beta] = \mathbb{Z}[\alpha]$, entonces disc $\alpha =$ disc β.

La propiedad (b) implica que disc α solo depende del subanillo $R = \mathbb{Z}[\alpha]$, por lo que tiene sentido escribir disc $R =$ disc α. Por el apartado (a), tenemos que subanillos más grandes de $\mathcal{O}$ tienen discriminante menor. En particular, disc $\mathcal{O}$ debe dividir a disc R para todo subanillo $R \subseteq \mathcal{O}$ de la forma $\mathbb{Z}[\alpha]$.

Definición 4.5. Denotamos como $D_F =$ disc $\mathcal{O} =$ disc δ_0 al **discriminante del cuerpo** $F = \mathbb{Q}[\sqrt{D}]$.

Vamos a resumir en una tabla la información básica del anillo de enteros $\mathcal{O}$ de $F = \mathbb{Q}[\sqrt{D}]$, con D libre de cuadrados:

D mod 4	δ_0, con $\mathcal{O} = Z[\delta_0]$	Ecuación para δ_0	$D_F =$ disc $\mathcal{O}$
2,3	$\sqrt{D}$	$\delta_0^2 - D = 0$	$4D$
1	$\frac{1+\sqrt{D}}{2}$	$\delta_0^2 - \delta_0 + \frac{1-D}{4} = 0$	D

Cuadro 1: Información sobre $\mathcal{O}$

Nota. Cabe remarcar que:

(a) disc $\mathcal{O}$ es siempre libre de cuadrados, salvo por un posible factor 4. Por la Proposición 4.2, esto es falso para el discriminante de cualquier subanillo $\mathbb{Z}[\alpha] \subset \mathcal{O}$. Este hecho será importante a la hora de probar la factorización única de ideales.

(b) Cuando probemos teoremas generales acerca de $\mathcal{O}$ no importa la elección de δ para $\mathcal{O} = \mathbb{Z}[\delta]$; cualquier δ con el discriminante correcto servirá, por tanto fijamos la siguiente notación:

(c) En caso de no querer distinguir entre los casos de la Tabla 1, en vez de δ_0 se puede utilizar

$$\delta_1 = \frac{D_F + \sqrt{D_F}}{2}, \text{ para el cual } \delta_1^2 - D_F\delta_1 + \frac{D_F^2 - D_F}{4} = 0.$$

Esta fórmula es algo más complicada, pero $\mathcal{O} = [\delta_1]$ independientemente del valor de D (mód 4).

Para el resto del trabajo, F denota un cuerpo cuadrático con discriminante D_F y anillo de enteros $\mathcal{O} = \mathbb{Z}[\delta]$. Tal δ cumple que $\delta^2 - t\delta + n = 0$, para ciertos $t, n \in \mathbb{Z}$ con $t^2 - 4n = D_F$.

Proposición 4.3. *Si $D_F < -4$, entonces $\mathcal{O}^\times = \{\pm 1\}$.*

Demostración. Como en la Proposición 1.5, $\epsilon = a + b\delta \in \mathcal{O}^\times$ si y solo si $N\epsilon = \pm 1$. Por la Proposición 4.1 (a), esto significa que $a^2 + tab + nb^2 = \pm 1$. Si $b = 0$, entonces $a^2 = 1$ y $\epsilon = \pm 1$. Si $b \neq 0$, dividimos por b y tenemos que

$$\left(\frac{a}{b}\right)^2 + t\left(\frac{a}{b}\right) + n = \pm\frac{1}{b^2}.$$

Si $D_F < -4$, esta ecuación no tiene solución en $\mathbb{Z}$, ya que $-D_F/4 > 1 \geq \pm 1/b^2$, porque $-D_F/4$, al ser la altura del vértice de la parábola, es el mínimo valor que toma la función $x^2 + tx + n$ en $\mathbb{R}$. □

4.3. Anillos Noetherianos

Identificamos $\mathcal{O}$ con el retículo estándar Λ_0 mediante el isomorfismo de grupo

$$x + y\delta \leftrightarrow \begin{bmatrix} x \\ y \end{bmatrix}.$$

Proposición 4.4. *El isomorfismo anterior identifica un ideal $I \neq 0$ de $\mathcal{O}$ con un subretículo de Λ_0.*

Demostración. Supongamos que existe un ideal $I \neq 0$ de $\mathcal{O}$ que no se corresponde com un subretículo. Por la clasificación de subgrupos de Λ_0 en el Teorema 3.1, I debe corresponderse con un subgrupo de la forma $\mathbb{Z}t$. Sea $\tau \in I$ el elemento correspondiente al generador t, entonces $\delta I \subseteq I$ para cada $\delta \in \mathcal{O}$ implica que $\delta\tau \in \mathbb{Z}\tau$, es decir, $\delta\tau = n\tau$ para cierto $n \in \mathbb{Z}$. Esto es una igualdad en F, por lo que podemos cancelar τ y concluir que $\delta = n$, lo que es una contradicción. □

Proposición 4.5. *Sea $I \neq 0$ un ideal de $\mathcal{O}$.*

(a) $\mathcal{O}/I$ es finito

(b) Cualquier cadena estrictamente ascendiente de ideales de $\mathcal{O}$ debe ser finita.

Demostración. Ambas se obtienen como resultado del estudio de retículos

(a) Se trata de un caso particular de la proposición 3.4.

(b) Una cadena estrictamente ascendiente de ideales de $\mathcal{O}$ es una secuencia (finita o infinita) de ideales tales que $I_1 \subset I_2 \subset \cdots \subset \mathcal{O}$. Tomamos el cociente de los ideales de la secuencia con I_1

$$0 = I_1/I_1 \subset I_2/I_1 \subset \cdots \subset \mathcal{O}/I_1.$$

Esto es una cadena estrictamente ascendente de subgrupos de $\mathcal{O}/I_1$, que por el apartado (a) tiene un número finito de subgrupos.

□

Corolario 4.2. *Todo ideal primo de $\mathcal{O}$ es maximal.*

Demostración. Se desprende directamente de la proposición 4.5 (a) y el criterio del corolario 2.2. □

Sea $\mathcal{S}$ una colección de ideales de $\mathcal{O}$ ordenados parcialmente por inclusión $\subseteq$. Decimos que un ideal $I \in \mathcal{S}$ es un elemento maximal de $\mathcal{S}$ si no está contenido en ningún otro ideal de $\mathcal{S}$.

Corolario 4.3. *Todo conjunto $\mathcal{S}$ no vacío de ideales de $\mathcal{O}$ tiene un elemento maximal.*

Demostración. Supongamos que no existe ningún elemento maximal. Tomamos un ideal $I_1 \in \mathcal{S}$, que no es un elemento maximal, por tanto existe $I_2 \in \mathcal{S}$ tal que $I_1 \subset I_2$. Repitiendo este proceso obtenemos una cadena estrictamente ascendente infinita, lo que es una contradicción. □

Corolario 4.4. *Todo ideal $I \subset \mathcal{O}$ está contenido en un ideal maximal de $\mathcal{O}$.*

Demostración. Obtenemos este resultado aplicando el corolario anterior al conjunto no vacío $\{J : J \text{ es ideal de } \mathcal{O} \text{ e } I \subseteq J \subset \mathcal{O}\}$. □

El resultado anterior se puede probar para cualquier anillo mediante el Lema de Zorn, estudiado en la asignatura *Estructuras Algebraicas*.

Definición 4.6. Un anillo R se dice **Noetheriano** si satisface que toda cadena de ideales estrictamente ascendiente es finita.

4.4. Forma estándar de un ideal

Dado un subretículo $\Lambda \subseteq \Lambda_0$, usamos la reducción por columnas para obtener $\Lambda = \gamma\Lambda_0$ para una matriz γ particularmente simple. Después de identificar $\mathcal{O}$ con Λ_0, este procedimiento nos permite describir explicitamente los ideales de $\mathcal{O}$.

Proposición 4.6. *Para cualquier ideal $I \subseteq \mathcal{O}$, existen $a, b, d \in \mathbb{Z}$ tales que*

(a) $I = d(\mathbb{Z}a + \mathbb{Z}(-b + \delta))$, *y*

(b) $b^2 - tb + n \equiv 0 \pmod{a}$*, o, equivalentemente,* $a \mid N(-b+\delta)$.

Inversamente, todo $I \in \mathcal{O}$ *cumpliendo (a) y (b) es un ideal.*

La expresión en (a) se conoce como forma estándar del ideal I. Tal expresión es única si forzamos que $d < 0$ y $0 \leq b < a$. Esto se probará en el Ejercicio 4.2, al final del capítulo.

Demostración. Como hemos visto, todo ideal I está relacionado mediante un isomorfismo con un subretículo $\Lambda = \gamma\Lambda_0$. Reduciendo γ por columnas, obtenemos $a', b', d \in \mathbb{Z}$ tales que

$$\Lambda = \begin{bmatrix} a' & b' \\ 0 & d \end{bmatrix} \Lambda_0 = \mathbb{Z}\begin{bmatrix} a' \\ 0 \end{bmatrix} + \mathbb{Z}\begin{bmatrix} b' \\ d \end{bmatrix}, \text{ y correspondientemente, } I = \mathbb{Z}a' + \mathbb{Z}(b' + d\delta).$$

Ahora, teniendo en cuenta que I absorbe la multiplicación por δ, lo aplicamos a la base $\{a', b' + d\delta\}$ de I para probar las dos condiciones de la proposición.

(a) Como I es un ideal, $\delta a' \in I$, luego existen $h, k \in \mathbb{Z}$ tales que

$$\delta a' = ha' + k(b' + d\delta) = (ha' + kb') + kd\delta.$$

Concluimos que $a' = kd$ y $ha' + kb' = 0$. Poniendo $a = k, b = h$ nos da $b' = -bd$, y, como buscábamos,

$$I = \mathbb{Z}da + \mathbb{Z}(-bd + d\delta) = d(\mathbb{Z}a + \mathbb{Z}(-b + \delta)).$$

(b) Es suficiente probar la parte (b) en el caso $d = 1$. Como $\delta I \subseteq I$, tenemos que $\delta(-b+\delta) = -b\delta + \delta^2 = -n + (t - b)\delta \in I$, la última igualdad se obtiene de $\delta^2 - t\delta + n = 0$. Así, existen $j, l \in \mathbb{Z}$ con

$$-n + (t - b)\delta = ja + l(-b + \delta) = (ja - lb) + l\delta.$$

Comparando las partes irracionales y racionales obtenermos que $-n = ja - lb$ y $t - b = l$. Multiplicando la segunda igualdad por $-b$ nos da $b^2 - tb = -lb = -ja - n$. Esto prueba la conguencia que buscábamos,

$$b^2 - tb + n = -ja \equiv 0 \pmod{a}.$$

Por la proposición 4.1 (a), la parte de la izquierda es $\mathrm{N}(-b + \delta)$. Para el inverso, invertimos estos cálculos para probar que $\delta I \subseteq I$.

□

Ejemplo 4.1. Vamos a ilustrar la proposición con un ejemplo. Sean $\mathcal{O} = \mathbb{Z}[i]$, $I = \mathcal{O}(2+i) = (\mathbb{Z}+\mathbb{Z}i)(2+i) = \mathbb{Z}(2+i)+\mathbb{Z}(-1+2i)$. Para pasar a forma estándar, reducimos por columnas:

$$\begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix} \to \begin{bmatrix} 2 & -5 \\ 1 & 0 \end{bmatrix} \to \begin{bmatrix} 5 & 2 \\ 0 & 1 \end{bmatrix}.$$

Una forma estándar de I es $\mathbb{Z} \cdot 5 + \mathbb{Z}(2 + i)$. La Figura 2 muestra dos paralelogramos fundamentales del retículo I, uno correspondiente a la base inicial $\{2 + i, -1 + 2i\}$, el otro a la base $\{5, 2 + i\}$ de la forma estándar.

Ambos paralelogramos fundamentales contienen cinco puntos de $\mathbb{Z}[i]$ (sin contar las líneas de puntos ni sus vértices), coincidiendo con $|\mathcal{O}/I| = 5$, y la norma del generador $(2 + i)$. Como podemos ver en el Ejercicio 4.1, al final del capítulo, no se trata de una coincidencia.

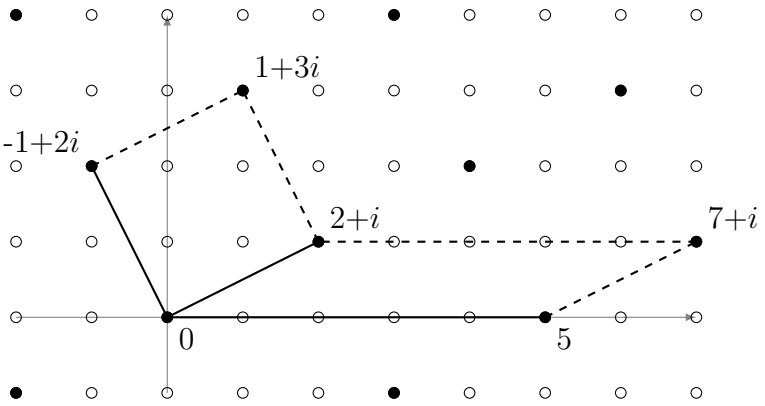

Figura 2: Forma estándar del ideal $I = \mathbb{Z}[i](2+i)$. Todos los puntos son elementos de $\mathbb{Z}[i]$, los puntos en negrita son también elementos de I.

4.5. Norma de un Ideal

Vamos a extender la noción de norma de elementos de F a ideales de $\mathcal{O}$. Por el Ejercicio 4.1, $|\mathrm{N}\alpha| = |\mathcal{O}/\mathcal{O}\alpha|$ para cualquier $\alpha \in \mathcal{O}$. También sabemos que $\mathcal{O}/I$ es finito para cualquier ideal $I \neq 0$. Todo ello propicia la siguiente definición.

Definición 4.7. La **norma** de un ideal $I \neq 0$ de $\mathcal{O}$ es $\mathrm{N}I = |\mathcal{O}/I|$.

La norma de los ideales es esencial para transformar cuestiones sobre multiplicación y división de ideales en cuestiones análogas pero más sencillas sobre números naturales.

Proposición 4.7. *Sean $I, J \neq 0$ dos ideales de $\mathcal{O}$. Si $I \mid J$, entonces $NI \mid NJ$.*

Demostración. $I \mid J$ simplemente significa que $I \supseteq J$, luego la asignación $\alpha + J \mapsto \alpha + I$ es un homomorfismo suprayectivo bien definido $\varphi : \mathcal{O}/I \to \mathcal{O}/J$. Por el Primer Teorema de Isomorfía, $\mathcal{O}/I \cong (\mathcal{O}/J)/\ker\varphi$. Contando elementos, tenemos que $|\mathcal{O}/I| \cdot |\ker\varphi| = |\mathcal{O}/J|$, luego $\mathrm{N}I = |\mathcal{O}/I|$ divide a $\mathrm{N}J = |\mathcal{O}/J|$ □

Ejemplo 4.2. Veamos que los ideales $I = \mathbb{Z}\cdot 11 + \mathbb{Z}(3+\sqrt{31})$, $J = \mathbb{Z}\cdot 6 + Z(1+\sqrt{31})$ de $\mathbb{Z}[\sqrt{31}]$ son coprimos. Dado que $I+J$ divide a I y a J, $\mathrm{N}(I+J) \mid$ m.c.d.($\mathrm{N}I$,$\mathrm{N}J$)=m.c.d.$(11,6) = 1$, luego $I + J = \mathbb{Z}[\sqrt{31}]$.

Teorema 4.2. *Sea $I \neq 0$ un ideal de $\mathcal{O}$ e $\bar{I} = \{\bar{\alpha} : \alpha \in I\}$. Entonces $I\bar{I} = \mathcal{O}\cdot NI$, el ideal principal generado por NI.*

Demostración. Sabemos que para todo I existen $a, b, d, j \in \mathbb{Z}$, $a, d \neq 0$, tales que

$$I = d(\mathbb{Z}a + \mathbb{Z}(-b+\delta)), b^2 - tb + n = ja.$$

Sea $I' = \mathbb{Z}a + \mathbb{Z}(-b+\delta)$, tenemos que

$$I\bar{I} = dI'(d\bar{I'}) = d^2(I'\bar{I'}) = (Nd)(I'\bar{I'}).$$

Es por tanto suficiente probar el teorema para I', luego asumimos $d = 1$. Por la Definición 4.2, $\bar{\delta} = t - \delta$, por tanto $I\bar{I} = (\mathbb{Z}a + \mathbb{Z}(-b+\delta))(\mathbb{Z}a + \mathbb{Z}(-b+t-\delta))$. Multiplicamos los ideales como vimos en el Capítulo 3 y tenemos que $I\bar{I}$ es una extensión $\mathbb{Z}$-lineal del conjunto

$$\{a^2, \quad -ab + a\delta, \quad -ab + at - a\delta, \quad b^2 - tb + n\}.$$

Para encontrar una base aplicamos la reducción por columnas, (teniendo en cuenta que $b^2 - tb + n = ja$) a

$$\begin{bmatrix} a^2 & -ab & -ab+at & ja \\ 0 & a & -a & 0 \end{bmatrix} \to \begin{bmatrix} a^2 & ja & 2ab-at & -ab \\ 0 & 0 & 0 & a \end{bmatrix}$$

Debemos reducir ahora la submatriz 1×3 $[a^2 \ \ ja \ \ 2ab-at]$. Dado que aplicar la reducción por columnas a una única fila es equivalente a aplicar el algoritmo de Euclides sucesivamente a las entradas de la fila, tenemos que $[0 \ \ 0 \ \ m.c.d.(a^2, ja, 2ab-at)]$.

Veamos que m.c.d.$(a^2, ja, 2ab-at)$=a, es decir, que m.c.d.$(a, j, 2b-t)$=1. Si p fuera un primo dividiendo a $a, j, 2b-t$, entonces

$$p^2 \mid (2b-t)^2 - 4ja = 4b^2 - 4bt + t^2 - 4b^2 + 4bt - 4n = t^2 - 4n = D_F.$$

Como D_F es libre de cuadrados salvo un posible factor 4, entonces $p = 2$. Si 2=m.c.d.$(a, j, 2b-t) \Rightarrow 2 \mid a, 2 \mid j, 2 \mid t$. Pero t =Tr δ y Tr $\delta \in \{0, 1\}$. Por tanto, tenemos que $t = 0$ y $D \equiv 2, 3$ (mód 4). En este caso, $t = 0$ y $n = -D$, siendo $\delta = \sqrt{D}$. Entonces, $b \in \mathbb{Z}$ cumple que $b^2 - D = ja$ (ya que b verifica $b^2 - tb + n = ja$). Así que como $2 \mid j, 2 \mid a$, se tiene que $b^2 \equiv D$ (mód 4), es decir, $b^2 \equiv 2, 3 \pmod 4$, contradicción. Luego

$$\begin{bmatrix} a^2 & ja & 2ab-at & -ab \\ 0 & 0 & 0 & a \end{bmatrix} \to \begin{bmatrix} 0 & 0 & a & -ab \\ 0 & 0 & 0 & a \end{bmatrix} \to \begin{bmatrix} 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{bmatrix}.$$

Concluimos por tanto que $I\bar{I} = \mathbb{Z}a + \mathbb{Z}a\delta = \mathcal{O}a = \mathcal{O}\cdot \mathrm{N}I$, ya que $\mathrm{N}I = |\mathcal{O}/I| = |\det \begin{bmatrix} a & -b \\ 0 & 1 \end{bmatrix}| = a$. □

La prueba del resultado anterior se basa en que D_F =disc$\mathcal{O}$ es esencialmente libre de cuadrados. Esto no se cumple para el discriminante de ningún subanillo $\mathbb{Z}[\alpha] \subset \mathcal{O}$, por la Proposición 4.2. Es por ello que $\mathcal{O}$ es el sitio adecuado en el que buscar la factorización única de ideales.

Corolario 4.5. *Sean $I, J \neq 0$ dos ideales de $\mathcal{O}$, $N(IJ)$ =$NI\,NJ$.*

Demostración. La demostración se desprende directamente del Teorema anterior. $IJ \cdot \overline{IJ} = \mathcal{O}\cdot \mathrm{N}(IJ)$. Por otra parte $I\bar{I} \cdot J\bar{J} = (\mathcal{O}\cdot \mathrm{N}I)(\mathcal{O}\cdot \mathrm{N}J) = \mathcal{O} \cdot (\mathrm{N}I \ \mathrm{N}J)$ □

Tenemos ya las herramientas suficientes para probar la cancelación en la multiplicación de ideales.

Corolario 4.6. *Sean I, J, K ideales de $\mathcal{O}$, con $I \neq 0$. Si $IJ = IK$, entonces $J = K$.*

Demostración.

$$IJ = IK \Rightarrow (I\bar{I})J = (I\bar{I})K \Rightarrow (NI)J = (NI)K \Rightarrow J = K.$$

□

4.6. Ideales fraccionarios

El producto de ideales es una operación asociativa y conmutativa en el conjunto $\mathbb{I}_F^+$ de los ideales de $\mathcal{O}$ distintos de 0. El único elemento invertible de $\mathbb{I}_F^+$ es la identidad $\mathcal{O}$. Apesar de ser pobre en inversos, $\mathbb{I}_F^+$ satisface la propiedad de la cancelación. Por tanto vamos a añadir a $\mathbb{I}_F^+$ los inversos de todos los ideales distintos de 0 para construir el grupo $\mathbb{I}_F$. Por el Teorema 4.2, $I\bar{I} = \mathcal{O}\cdot \mathrm{N}I$, lo que nos invita a considerar $I^{-1} = (1/\mathrm{N}I)\cdot \bar{I}$.

Ejemplo 4.3. Sea $I = \mathbb{Z}[i]\cdot 2$ un ideal de $\mathbb{Z}[i]$. Con la definición (provisional) anterior, $I^{-1} = \mathbb{Z}[i]\cdot 1/2 = \mathbb{Z}\cdot 1/2 + \mathbb{Z}\cdot i/2$, que es un retículo, pero no está contenido en $\mathbb{Z}[i]$.

Un ideal I de $\mathcal{O}$ es un subgrupo que absorbe la multiplicación por $\mathcal{O}$. Llegamos a la idea de un ideal fraccionario eliminando la condición $I \subseteq \mathcal{O}$.

Definición 4.8. Un **ideal fraccionario** en F es un subgrupo aditivo $\mathscr{I}$ de F que satisface las dos condiciones siguientes :

(a) $\mathscr{I} = \mathbb{Z}\alpha + \mathbb{Z}\beta$, donde $\alpha, \beta \in F$ son linealmente independientes sobre $\mathbb{Z}$.

(b) $\delta\mathscr{I} \subseteq \mathscr{I}$.

Denotamos al conjunto de todos los ideales fraccionarios como $\mathbb{I}_F$.

Nota. Un ideal fraccionario contenido en $\mathcal{O}$ es simplemente un ideal de $\mathcal{O}$, es decir, $\mathbb{I}_F^+ \subseteq \mathbb{I}_F$. Para enfatizar, a veces nos referiremos a estos ideales como **ideales enteros**.

Ejemplo 4.4. Para cualquier $\alpha \in F\backslash 0$, el conjunto

$$\mathcal{O}\alpha = \{\beta\alpha : \beta \in \mathcal{O}\} = \mathbb{Z}\alpha + \mathbb{Z}\delta\alpha$$

es un ideal fraccionario. Los ideales fraccionarios de esta forma se denominan **ideales fraccionarios principales**.

Proposición 4.8. *Un subconjunto $\mathscr{I} \subseteq F$ es un ideal fraccionario si y solo si existe $e \neq 0 \in \mathbb{Z}$ tal que $e\mathscr{I}$ es un ideal de $\mathcal{O}$.*

Demostración. Sea $\mathscr{I} = \mathbb{Z}\alpha + \mathbb{Z}\beta$. Tomando el común denominador, podemos encontrar $a, b, c, d, e \in \mathbb{Z}$ para los cuales $\alpha = (a + b\sqrt{D})/e, \beta = (c + d\sqrt{D})/e$. Multiplicando por e eliminamos los denominadores, luego $e\mathscr{I} \subseteq \mathcal{O}$. $e\mathscr{I}$ no es solo un subgrupo de $\mathcal{O}$, ya que $\delta(e\mathscr{I}) = e(\delta\mathscr{I}) \subseteq e\mathscr{I}$, por tanto es un ideal de $\mathcal{O}$. El recíproco es trivial. □

Nos referiremos a cualquier e como el de la Proposición anterior como **denominador** (entero) de $\mathscr{I}$. Combinando las Proposiciones 4.6 y 4.8 obtenemos la siguiente afirmación.

Corolario 4.7. *Los ideales fraccionarios son los subconjuntos de F de la forma $q(\mathbb{Z}a + \mathbb{Z}(-b+\delta))$ para ciertos $q \in \mathbb{Q}^\times$ y $a, b \in \mathbb{Z}$ tales que $a \neq 0$ y $b^2 - tb + n \equiv 0 \pmod{a}$.*

Ahora que ya tenemos una descripción explícita de sus elementos, vamos a proceder a definir una estructura de grupo en $\mathscr{I}_F$.

Proposición 4.9. *Sean $\mathscr{I}, \mathscr{J} \in \mathbb{I}_F$ y $k, l \in \mathbb{Z}$ tales que $k\mathscr{I}, l\mathscr{J} \subseteq \mathcal{O}$. La fórmula*

$$\mathscr{I} \cdot \mathscr{J} = \frac{1}{kl}(k\mathscr{I})(l\mathscr{J})$$

da una operación bien definida en $\mathbb{I}_F$ extendiendo la multiplicación de ideales usual en $\mathbb{I}_F^+$. Bajo esta operación, $\mathbb{I}_F$ es un grupo abeliano. Es más, la norma de un ideal se extiende a un homomorfismo de grupos multiplicativos $\mathbb{I}_F \to \mathbb{Q}_{>0}^\times$ como $N(\frac{1}{e}I) = \frac{1}{e^2}NI$, $e \in \mathbb{Z}, I \in \mathbb{I}_F^+$.

Demostración. Sean $k', l' \in \mathbb{Z}$ otro par de denominadores de $\mathscr{I}$ y $\mathscr{J}$ respectivamente. Entonces $kk'\mathscr{I} \subseteq \mathcal{O}$ y $ll'\mathscr{J} \subseteq \mathcal{O}$ también. Por la asociatividad y conmutatividad de la multiplicación usual de ideales, se tiene que

$$(k'l')(k\mathscr{I})(l\mathscr{J}) = (kk'\mathscr{I})(ll'\mathscr{J}) = (kl)(k'\mathscr{I})(l'\mathscr{J}).$$

Multiplicando por $1/kk'll'$, tenemos que

$$\frac{1}{kl}(k\mathscr{I})(l\mathscr{J}) = \frac{1}{k'l'}(k'\mathscr{I})(l'\mathscr{J}),$$

por tanto, el producto de ideales fraccionarios no depende de la elección de denominadores.

Esta operación extiende la multipliación en $\mathbb{I}_F^+$, y es también asociativa y conmutativa, con identidad $\mathcal{O}$. Queda por probar la existencia de inversos. Tomamos $\mathscr{I} \in \mathbb{I}_F$ y $e \in \mathbb{Z}$ con $e\mathscr{I} \subseteq \mathcal{O}$. Por el Teorema 4.2, $(e\mathscr{I})(e\bar{\mathscr{I}}) = \mathcal{O}\cdot\mathrm{N}(e\mathscr{I})$, luego $\mathscr{I} \cdot (e^2/\mathrm{N}(e\mathscr{I}) \cdot \bar{\mathscr{I}}) = \mathcal{O}$, por tanto

$$\mathscr{I}^{-1} = \frac{e^2}{N(e\mathscr{I})} \cdot \bar{\mathscr{I}}.$$

La afirmación sobre la norma se obtiene teniendo en cuenta que para todo $\mathscr{I} \in \mathbb{I}_F$ se tiene que $\mathscr{I} = \frac{1}{e}I$ para cierto $I \in \mathcal{O}$. □

La construcción de $\mathbb{I}_F$ a partir de $\mathbb{I}_F^+$ es análoga a la ampliación de $\mathbb{N}$ con sus inversos para construir los racionales positivos.

4.7. Factorización Única de Ideales

Finalmente, estamos preparados para probar la existencia de la factorización única para ideales.

Teorema 4.3. *Sea $F = \mathbb{Q}[\sqrt{D}]$ un cuerpo cuadrático y $\mathcal{O}$ su anillo de enteros. Para cualquier ideal I de $\mathcal{O}$, distinto de 0 y $\mathcal{O}$, existen ideales primos $P_1, P_2, \ldots, P_n$ de $\mathcal{O}$, no necesariamente distintos, tales que $I = P_1P_2\cdots P_n$. Esta factorización es única salvo permutación de los factores.*

Demostración. Existencia: Sea $\mathcal{S}$ el conjunto de todos los ideales $0 \subset I \subset \mathcal{O}$ sin una factorización prima. Supongamos que $\mathcal{S}$ no es vacío. Por la Proposición 4.5, $\mathcal{O}$ es un anillo Noetheriano, luego, por el Corolario 4.3, existe un elemento maximal $L \in \mathcal{S}$. El ideal L no puede ser primo, ya que cada ideal primo es su propia factorización. Por tanto, por el Corolario 4.2, L tampoco es un ideal maximal, luego L está contenido estrictamente contenido en un ideal maximal P por el Corolario 4.4: $L \subset P \subset \mathcal{O}$.

La multiplicación de ideales fraccionarios preserva inclusiones estrictas: si $J \subset K$ pero $IJ = IK$, cancelando I tenemos una contradicciñon $J = K$. Así, multiplicando $L \subset P$ por P^{-1} nos da $LP^{-1} \subset \mathcal{O}$. Similarmente, $P \subset \mathcal{O}$ implica que $\mathcal{O} \subset P^{-1}$, y multiplicando por L, $L \subset LP^{-1}$.

Es decir, $LP^{-1} \neq \mathcal{O}$ es un ideal entero estrictamente más grande que L, y por tanto, no está en $\mathcal{S}$. Así, tenemos una factorización prima $LP^{-1} = P_1 \cdots P_k$, pero entonces $L = P_1 \cdots P_k P$ es una factorización prima de L, contradiciendo $L \in \mathcal{S}$. Por tanto $\mathcal{S}$ es el conjunto vacío; todo ideal no trivial de $\mathcal{O}$ tiene una factorización prima.

Unicidad: Sea $I = P_1 \cdots P_r = Q_1 \cdots Q_s$. Entonces $P_1 \mid Q_1 \cdots Q_s$. Por la versión para ideales del Lema de Euclides (Ejercicio 2.1) tenemos que P_1 divide a uno de los factores de la derecha. Pongamos que tal ideal es Q_1 ($P_1 \supseteq Q_1$). Por el Corolario 2.2, todo ideal primo distinto de 0 en $\mathcal{O}$ es un ideal maximal, luego $P_1 = Q_1$. Por el Corolario 4.6, podemos cancelar P_1, Q_1 para obtener $P_2 \cdots P_r = Q_2 \cdots Q_s$. Procediendo de manera inductiva, emparejamos cada P_i con un Q_j, luego una factorización prima de I es una permutación de la otra. □

4.8. Ideales Primos en $\mathcal{O}$

Antes de empezar a factorizar ideales, necesitamos una descripción explícita de los ideales primos.

Lema 4.1. *Sea $P \neq 0$ un ideal primo de $\mathcal{O}$. Existe un único $p \in \mathbb{N}$ tal que $P \mid p$.*

Demostración. Sea $\mathrm{N}P = pp' \ldots$ la factorización prima en $\mathbb{N}$ de $\mathrm{N}P$. El ideal P es primo, y divide a $P\bar{P} = \mathcal{O} \cdot \mathrm{N}\ P = (\mathcal{O}p)(\mathcal{O}p') \ldots$. Por el Lema de Euclides para ideales, Ejercicio 2.1, tenemos que $P \mid p$ (salvo reordenamiento). Por tanto $\mathrm{N}P \mid \mathrm{N}p = p^2$, luego $p \in \mathbb{N}$ debe ser el único factor primo de $\mathrm{N}P$. □

Para encontrar todos los ideales primos distintos de 0 de $\mathcal{O}$, basta con factorizar el ideal $\mathcal{O}p$ para cada primo $p \in \mathbb{N}$. Sea $\mathcal{O}p = P_1 P_2 \ldots$ esa factorización, tomando la norma tenemos que

$$p^2 = \mathrm{N}(\mathcal{O}p) = (\mathrm{N}P_1)(\mathrm{N}P_2) \ldots$$

lo que nos deja unicamente tres posibilidades.

Proposición 4.10. *Sea $p \in \mathbb{N}$ un primo. La factorización de $\mathcal{O}p$ tiene una de las siguientes formas:*

*(a) $\mathcal{O}p = P$ con $NP = p^2$; es decir, p, visto como un ideal principal de $\mathcal{O}$, sigue siendo primo. Decimos que p es **inerte**.*

*(b) $\mathcal{O}p = P^2$ con $NP = p$. Decimos que p es **se ramifica**.*

*(c) $\mathcal{O}p = P\bar{P}$ con $NP = p$ y $P \neq \bar{P}$. Decimos que p es **se escinde**.*

Los términos *inerte*, *ramificado* y *dividido* también se aplican a los ideales primos $P, \bar{P}$ factores de $\mathcal{O}p$.

Demostración. Sea P un ideal primo factor de $\mathcal{O}p$. Si $\mathrm{N}P = p^2$, estamos en el caso (a). En caso contrario, $\mathcal{O}p = \mathcal{O}\cdot\mathrm{N}P = P\bar{P}$ es la única fatorización prima de $\mathcal{O}p$. Si $P = \bar{P}$, estamos en el caso (b); si no, en el caso (c). □

Proposición 4.11. *Sea $p \in \mathbb{N}$ un primo, y sea $\nu = 0, 1$ o 2 el número de soluciones distintas en $\mathbb{Z}/p\mathbb{Z}$ de la ecuación $x^2 - tx + n = 0$. Entonces el tipo de factorización prima de $\mathcal{O}p$ queda determinado por ν:*

(a) $\nu = 0$ si y solo si p es inerte.

(b) $\nu = 1$ si y solo si p se ramifica.

(c) $\nu = 2$ si y solo si p se escinde.

Demostración. Dado que una ecuación cuadrática tiene a lo sumo dos soluciones en el cuerpo $\mathbb{Z}/p\mathbb{Z}$ es sufieciente con probar unicamente la dirección "si" en cada uno de los tres casos.

(a): Supongamos que p es inerte y que existe un $r \in \mathbb{Z}$ tal que $r^2 - tr - n \equiv 0 \pmod{p}$. Entonces $(r-\delta)(r-\bar{\delta}) = r^2 - tr + n \in \mathcal{O}p$. El ideal $\mathcal{O}p$ es primo, luego debe contener a uno de los factores, pongamos $r - \delta$. Pero entonces $r/p - \delta/p \in \mathcal{O}$, lo que es una contradicción.

(b) y (c): Supongamos que $\mathcal{O}p = P\bar{P}$, lo que describe tanto el caso en que se ramifica como en el que se escinde, según sea $P = \bar{P}$ o no. Sea $P = d(\mathbb{Z}a + \mathbb{Z}(-b+\delta))$ la forma estándar de P. Entonces $p = \mathrm{N}P = d^2a$, luego $d = 1, a = p$ y

$$P = \mathbb{Z}p + \mathbb{Z}(-b+\delta),$$

$$\bar{P} = \ p + \mathbb{Z}(-b+\bar{\delta}) = \mathbb{Z}p + \mathbb{Z}(b-t+\delta).$$

Como $\bar{\delta} - (t-b) = -(t-\bar{\delta}) + b = -\delta + b \in P$, tenemos que

$$x^2 - tx + n = (x-\delta)(x-\bar{\delta}) \equiv (x-b)(x-(t-b)) \pmod{P}.$$

Dado que b y $t-b$ están ambos en $\mathbb{Z}$, módulo p ambos ambos acabarán estando en $\mathbb{Z}/p\mathbb{Z}$. Tenemos que $\nu = 1$ si y solo si $b \equiv t - b \pmod{p}$, y si no $\nu = 2$. La última congruencia es también una condición suficiente y necesaria para que P se ramifique. En efecto, la condición $P = \bar{P}$ es equivalente a la condición más débil $P \subseteq \bar{P}$, o

$$(\mathbb{Z}p + \mathbb{Z}(-b+\delta)) \subseteq (\mathbb{Z}p + \mathbb{Z}(b-t+\delta)).$$

Esto es equivalente a la existencia de $k, l \in \mathbb{Z}$ tales que $-b+\delta = kp + l(b-t+\delta)$. Comparando coeficientes, observamos que esto ocurre si y solo si $l = 1, -b = kp + b - t$, o, equivalentemente, $b \equiv t - b \pmod{p}$. □

Proposición 4.12. *El número de soluciones de la ecuación $x^2 - tx + n = 0$ en $\mathbb{Z}/p\mathbb{Z}$ es $\nu = 1 + \left(\frac{D_F}{p}\right)$.*

Demostración. Asumamos que $p > 2$, luego 2 es invertible en $\mathbb{Z}/p\mathbb{Z}$. Esto nos permite dividir por 2 cuando completemos cuadrados como en la demostración estándar de la fórmula cuadrática:

$$0 = x^2 - tx + n = (x - t/2)^2 - \frac{t^2 - 4n}{4},$$

multiplicando por 4 a ambos lados, $(2x-t)^2 = D_F$. El número de soluciones ν depende por tanto de si D_F es un cuadrado en módulo p, lo cual viene determinado por el símbolo de Legendre, de la Definición 1.2:

$$\nu=\begin{cases}0 \text{ si } D_F \text{ no es un cuadrado en } \mathbb{Z}/p\mathbb{Z}\\ 1 \text{ si } D_F=0 \pmod p\\ 2 \text{ si } D_F \text{ es un cuadrado distinto de 0 en } \mathbb{Z}/p\mathbb{Z}\end{cases} = 1+\left(\frac{D_F}{p}\right).$$

Si $p=2$ no podemos completar el cuadrado. Se trata este caso en el Ejercicio 4.4, al final del Capítulo. □

Resumimos los resultados previos en esta ultima afirmación acerca de factorización en $\mathcal{O}$.

Teorema 4.4. *Sea $p \in \mathbb{N}$ un primo.*

(a) Si $\left(\frac{D_F}{p}\right)=-1$, $\mathcal{O}p$ es un ideal primo en $\mathcal{O}$: p es inerte.

(b) Si $\left(\frac{D_F}{p}\right)=0$ o 1, tomamos $b \in \mathbb{Z}$ tal que $b^2-tb+n \equiv 0 \pmod p$. Sea $P=\mathbb{Z}p+\mathbb{Z}(-b+\delta)$, entonces se cumple que:

- *P es un ideal primo en $\mathcal{O}$.*
- *$\bar{P}=\mathbb{Z}p+\mathbb{Z}(-(t-b)+\delta)$.*
- *Se da la siguiente factorización en ideales primos $\mathcal{O}p=P\bar{P}$.*
- *$\left(\frac{D_F}{p}\right)=0$ si y solo si $P=\bar{P}$, o, equivalentemente, si $b \equiv t-b \pmod p$: p se ramifica.*
- *$\left(\frac{D_F}{p}\right)=1$ si y solo si $P \neq \bar{P}$, o, equivalentemente, si $b \not\equiv t-b \pmod p$: p se escinde.*

Dado que $\left(\frac{D_F}{p}\right)=0$ si y solo si $p \mid D_F$, obtenemos el siguiente corolario.

Corolario 4.8. *Un primo $p \in \mathbb{N}$ se ramifica si y solo si $p \mid D_F$. En particular, solo un número finito de primos en $\mathbb{N}$ son ramificados.*

Ejemplo 4.5. Sea $F=\mathbb{Q}[\sqrt{-14}]$, luego $\mathcal{O}=\mathbb{Z}[\sqrt{-14}]$. Los únicos primos ramificados son 2 y 7, los divisores primos de $D_F=-56$. El elemento $\delta=\sqrt{-14}$ es una raíz de la ecuación $x^2+14=0$, que se reduce a $x^2=0$ tanto en módulo 2 como en 7. Podemos tomar $b=t-b=0$ en el Teorema 4.4 (b). Tenemos por tanto que $\mathcal{O}\cdot 2=P_2^2, \mathcal{O}\cdot 7=P_7^2$, donde

$$P_2=\mathbb{Z}\cdot 2+\mathbb{Z}\sqrt{-14} \text{ y } P_7=\mathbb{Z}\cdot 7+\mathbb{Z}\sqrt{-14}$$

son ideales primos de $\mathcal{O}$. Consideremos las factorizaciones de 11 y 23. Por reciprocidad cuadrática,

$$\left(\frac{-56}{11}\right)=\left(\frac{-1}{11}\right)=-1, \qquad \left(\frac{-56}{23}\right)=\left(\frac{-14}{23}\right)=\left(\frac{9}{23}\right)=1,$$

Luego 11 es inerte y 23 se escinde. De hecho, $(\pm 3)^2 \equiv -14 \pmod{23}$, y la receta en el Teorema 4.4 (b) nos da la factorización prima

$$\mathcal{O}\cdot 23=(\mathbb{Z}\cdot 23+\mathbb{Z}(-3+\sqrt{-14}))(\mathbb{Z}\cdot 23+\mathbb{Z}(3+\sqrt{-14})).$$

Ejemplo 4.6. Sea $F = \mathbb{Q}[\sqrt{-15}]$. Se tiene que $D_F = -15$ y $\mathcal{O} = \mathbb{Z}[\delta]$, donde $\delta = (1 + \sqrt{-15})/2$ satisfaciendo que $\delta^2 - \delta + 4 = 0$. Vamos a factorizar $I = \mathbb{Z}\cdot 84 + \mathbb{Z}(49 + 7\delta)$ en ideales primos. Primero, pongamos I en forma estándar factorizando por el $m.c.d.(84, 49, 7) = 7$:

$$I = 7(\mathbb{Z} \cdot 12 + \mathbb{Z}(7 + \delta)).$$

En la notación que hemos establecido, $d = 7, a = 12$ y $b = -7$. Dado que $(-7)^2 - (-7) + 4 = 60 \equiv 0 \pmod{12}$, I es en efecto un ideal. Por el Ejercicio 4.3, que se encuentra al final del Capítulo, su norma es $\mathrm{N}I = d^2 a = 2^2 \cdot 3 \cdot 7^2$. Primero calculamos la factorización de $2, 3$ y 7 en ideales primos en $\mathcal{O}$:

2: Dado que $x^2 - x + 4 \equiv x^2 + x \equiv x(x+1) \pmod{2}$, el primo 2 se escinde: $\mathcal{O}\cdot 2 = P_2\bar{P}_2 = (\mathbb{Z} \cdot 2 + \mathbb{Z}\delta)(\mathbb{Z} \cdot 2 + \mathbb{Z}(1 + \delta))$.

3: Es un divisor de D_F, luego se ramifica. Tenemos que $x^2 - x + 4 \equiv (x + 1)^2 \pmod{3}$, luego $\mathcal{O} \cdot 3 = P_3^2$ con $P_3 = \mathbb{Z} \cdot 3 + \mathbb{Z}(1 + \delta)$.

7: Como $\left(\frac{-15}{7}\right) = \left(\frac{6}{7}\right) = -1$, el ideal principal $\mathcal{O} \cdot 7$ es primo. En consecuencia, no hay ningún ideal de norma 7.

Vamos a factorizar I encontrando suficientes potencias de estos ideales primos, con las que obtener todas las potencias de primos que dividen $\mathrm{N}I$ en $\mathbb{N}$. El factor 7 de I tiene norma $\mathrm{N}(\mathcal{O} \cdot 7) = 7^2$, y así obtenemos todas las potencias de 7 en $\mathrm{N}I$. De forma similar, $3 \mid \mathrm{N}I$ y P_3 es el único ideal de norma 3, por tanto P_3 debe dividir a I.

Para conseguir el factor 2^2 en $\mathrm{N}I$, el ideal I debe tener dos factores ideales primos de norma 2 (posiblemente iguales). El producto de los dos puede ser $P_2^2, \bar{P}_2^{\,2}$ o $P_2\bar{P}_2 = \mathcal{O} \cdot 2$. Descartamos la última posibilidad, ya que observando la forma estándar de I, es obvio que $2 \nmid I$. Para decidir si $P_2^2 \mid I$ o $\bar{P}_2^{\,2} \mid I$, podríamos usar la fuerza bruta y calcular $I(P_2^2)^{-1} = \frac{1}{4} I \bar{P}_2^{\,2}$ y $I(\bar{P}_2^{\,2})^{-1} = \frac{1}{4} P_2^2$, y ver cual es un subconjunto de $\mathcal{O}$.

Podemos, sin embargo, evitar la multiplicación de ideales. Dado que $12 \in P_2$, tenemos que $P_2 \mid I$, es decir, $P_2 \supseteq I$, si y solo si $7 + \delta \in P_2$, y de forma análoga para $\bar{P}_2$. Calculamos $7 + \delta = 3 \cdot 2 + (1 + \delta) \in \bar{P}_2$, luego $\bar{P}_2 \mid I$. Finalmente obtenemos la factorización prima $I = 7 \cdot P_3 \cdot \bar{P}_2^{\,2}$.

Este ejemplo se generaliza en un algoritmo de factorización para ideales con $d = 1$. En combinación con el Teorema 4.4, nos permite factorizar explicitamente cualquier ideal.

Proposición 4.13. *Sea $I = \mathbb{Z}a + \mathbb{Z}(-b + \delta)$ un ideal de $\mathcal{O}$. Sea $a = p_1^{e_1} \cdots p_r^{e_r}$ la factorización prima de a en $\mathbb{Z}$. La factorización de I en ideales primos viene dada por*

$$I = \prod_{i=1}^{r} (\mathbb{Z}p_i + \mathbb{Z}(-b_i + \delta))^{e_i}.$$

donde $b_i^2 - tb_i + n \equiv 0 \pmod{p_i}$.

4.9. Ejercicios

Ejercicio 4.1. *Sea $\alpha \in \mathcal{O}$. Prueba que $|\mathcal{O}/\mathcal{O}\alpha| = |N\alpha|$.*

Sea $\alpha = a+b\delta$, con $a, b \in \mathbb{Z}$ y δ tal que $\delta^2 - t\delta + n = 0$. $\mathcal{O}\alpha = \mathbb{Z}(a+b\delta)+\mathbb{Z}(a\delta+b\delta^2) = \mathbb{Z}(a+b\delta)+\mathbb{Z}(a\delta+b(t\delta-n))$. Por la Proposición 3.4, $|\mathcal{O}/\mathcal{O}\alpha| = |\det\begin{bmatrix} a & -bn \\ b & a+bt \end{bmatrix}| = |a^2+abt+b^2n|$. Dependiendo de si $D \equiv 2,3 \pmod 4$ o $D \equiv 1 \pmod 4$, tenemos dos opciones. En primer lugar, $\mathrm{N}\alpha = a^2 - b^2D = a^2 + abt + b^2n$ ya que cuando $D \equiv 2,3 \pmod 4$, $\delta = \sqrt{D}$ y $t = 0, n = -D$. En segundo lugar, $\mathrm{N}\alpha = a^2 + ab + b^2(1-D)/4 = a^2 + abt + b^2n$ ya que cuando $D \equiv 1 \pmod 4$, $\delta = (1+\sqrt{D})/2$ y $t = 1, n = (1-D)/4$.

Ejercicio 4.2. *Sean $d(\mathbb{Z}a+\mathbb{Z}(-b+\delta)) = d'(\mathbb{Z}a'+\mathbb{Z}(-b'+\delta))$ dos formas estándar diferentes de un ideal $I \in \mathcal{O}$. Prueba que $d' = \pm d, a' = \pm a$, y $b' \equiv b \pmod a$.*

Dado que tanto da como $d'a'$ están contenidos en $\mathcal{O}$, tenemos que $da = md'a', m \in \mathbb{Z}$ y $d'a' = nda, n \in \mathbb{Z}$, por tanto $da = \pm d'a'$. Ahora, dado que ambas formas representan al mismo ideal I, tienen el mismo retículo Λ asociado. Sean $\gamma = \begin{bmatrix} da & -db \\ 0 & d \end{bmatrix}, \gamma' = \begin{bmatrix} \pm da & -d'b' \\ 0 & d' \end{bmatrix}$, $\Lambda = \gamma\Lambda_0 = \gamma'\Lambda_0$. Por la Proposición 3.4, $|\Lambda_0/\Lambda| = |\det\gamma| = |\det\gamma'|$, así, se tiene que $d^2a = \pm dad'$, luego $d = \pm d'$ y por tanto $a = \pm a'$. Veamos que $b' \equiv b \pmod a$. Tenemos que $d(-b'+\delta) = \pm mda \pm nd(-b+\delta), n, m \in \mathbb{Z}$. Vamos a probar uno de los cuatro posibles casos, el resto se realizan de manera análoga. Igualando las partes real y compleja tenemos que $d = nd \Rightarrow n = 1$ y por otra parte $-db' = mda - ndb = mda - db \Rightarrow b' = -ma + b \Rightarrow b' \equiv b \pmod a$.

Ejercicio 4.3. *Prueba que $NI = |d^2a|$ para un ideal $I = d(\mathbb{Z}a + \mathbb{Z}(-b+\delta))$ de $\mathcal{O}$.*

Como hemos visto anteriormente, en las Proposiciones 3.4 y 4.5, $\mathrm{N}I = |\mathcal{O}/I| = |\det\begin{bmatrix} da & -db \\ 0 & d \end{bmatrix}| = |d^2a|$.

Ejercicio 4.4. *Prueba la Proposición 4.12 cuando $p = 2$.*

Veamos en primer lugar que $D_F = t^2 - 4n$ en $\pmod 8$ depende unicamente de $n \pmod 2$ y $t \pmod 4$. Sea $n \equiv r_1 \pmod 2$ y $t \equiv r_2 \pmod 4$, entonces $t^2 - 4n = (4k_2 + r_2)^2 - 4(2k_1 + r_1) = 16k_2^2 + 8k_2r_2 + r_2^2 - 8k_1 - 4r_1 \equiv r_2^2 - 4r_1 \pmod 8$. Por tanto los posibles valores de $D_F \pmod 8$ son los siguientes:

	$t \equiv 0 \pmod 4$	$t \equiv 1 \pmod 4$	$t \equiv 2 \pmod 4$	$t \equiv 3 \pmod 4$
$n \equiv 0 \pmod 2$	0	1	4	1
$n \equiv 1 \pmod 2$	4	5	0	5

Vamos a completar ahora una tabla con las cuatro posiles ecuaciones cuadráticas con coeficientes en $\mathbb{Z}/2\mathbb{Z}$.

$x^2+tx+n\equiv 0 \pmod 2$	ν	$D_F \pmod 8$	$\left(\frac{D_F}{2}\right)$
$x^2\equiv 0 \pmod 2$	1	0	0
$x^2+x\equiv 0 \pmod 2$	2	1	1
$x^2+1\equiv 0 \pmod 2$	1	4	0
$x^2+x+1\equiv 0 \pmod 2$	0	5	-1

Cuando definimos el símbolo de Legendre, $\left(\frac{a}{p}\right)$, exigíamos que p fuera un primo positivo impar. Para $p=2$, utilizamos el símbolo de Kronecker, una ampliación del de Legendre (en el sentido de que ambos cumplen las mismas propiedades), para el cual $\left(\frac{a}{2}\right)$ se define como

$$\left(\frac{a}{2}\right)=\begin{cases}0 & \text{si } 2\mid a\\ 1 & \text{si } a\equiv \pm 1 \pmod 8\\ -1 & \text{si } a\equiv \pm 3 \pmod 8\end{cases}$$

Observando la tabla comprobamos que efectivamente, $\nu = 1+\left(\frac{D_F}{2}\right)$.

Ejercicio 4.5. *Factoriza el ideal principal generado por $5+\sqrt{-5}$ en ideales primos.*

En primer lugar, vamos expresar $\mathcal{O}(5+\sqrt{-5})$ de forma estándar. Para ello vamos a utilizar el método visto en en Capítulo 3 basado en la reducción de matrices.

$$\mathcal{O}(5+\sqrt{-5}) = (\mathbb{Z}+\mathbb{Z}\sqrt{-5})(5+\sqrt{-5})) = \mathbb{Z}(5+\sqrt{-5})+\mathbb{Z}(-5+5\sqrt{-5}).$$

Por tanto, tenemos que reducir la siguiente matriz:

$$\begin{bmatrix}5 & -5\\ 1 & 5\end{bmatrix}\to\begin{bmatrix}5 & -30\\ 1 & 0\end{bmatrix}\to\begin{bmatrix}-30 & 5\\ 0 & 1\end{bmatrix}\to\begin{bmatrix}30 & 5\\ 0 & 1\end{bmatrix}$$

Es decir, $\mathcal{O}(5+\sqrt{-5}))=\mathbb{Z}\cdot 30+\mathbb{Z}(5+\sqrt{-5})$, y $\mathrm{N}I=30=2\cdot 3\cdot 5$, luego $2,3,5$ son los únicos primos que están en I. $\sqrt{-5}$ es raíz de x^2+5, luego $t=0, n=5$.

Tenemos que $D_F=4D=-20$, luego, como $2\mid -20$ y $5\mid -20$, tenemos que 2 y 5 se ramifican, y por tanto, $\mathcal{O}\cdot 2=P_2^2$ y $\mathcal{O}\cdot 5=P_5^2$. Tomamos $b_2=-1$, ya que $b_2^2+5\equiv 0 \pmod 2$ y $b_5=0$, ya que $b_5^2+5\equiv 0 \pmod 5$, luego $P_2=\mathbb{Z}\cdot 2+\mathbb{Z}(1+\sqrt{-5}), P_5=\mathbb{Z}\cdot 5+\mathbb{Z}(\sqrt{-5})$.

Por otra parte, $x^2+5\equiv x^2+2\equiv (x-1)(x-2) \pmod 3$. Por tanto 3 se escinde y $\mathcal{O}\cdot 3=P_3\overline{P_3}$. Tomamos $b_3=1$, ya que $b_3^2+5\equiv 0 \pmod 3$, y por tanto $P_3=\mathbb{Z}\cdot 3+\mathbb{Z}(-1+\sqrt{-5})$ y $\overline{P_3}=\mathbb{Z}\cdot 3+\mathbb{Z}(1+\sqrt{-5})$.

Como $\mathrm{N}(P_2)=2$, $\mathrm{N}(P_3)=3$ y $\mathrm{N}(P_5)=5$, tenemos que $I=P_2\cdot P_3\cdot P_5$ o $I=P_2\cdot\overline{P_3}\cdot P_5$. Si $P_3\mid I$, entonces $I\subseteq P_3$. Dado que $5+\sqrt{-5}=6+(-1+\sqrt{-5})$, tenemos que $5+\sqrt{-5}\in P_3$, y $5+\sqrt{-5}\notin\overline{P_3}$; luego $\mathcal{O}(5+\sqrt{-5})=P_2\cdot P_3\cdot P_5$.

Ejercicio 4.6. *Sea $\mathscr{I}$ un ideal fraccionario de F. Prueba que $\mathscr{I}^{-1}=\{\alpha\in F:\alpha\mathscr{I}\subseteq\mathcal{O}\}$.*

Sea $\mathscr{J}=\{\alpha\in F:\alpha\mathscr{I}\subseteq\mathcal{O}\}$, es obvio que $\mathscr{J}\mathscr{I}\subseteq\mathcal{O}$. Hemos definido anteriormente $\mathscr{I}^{-1}=\frac{e\bar{I}}{N(I)}$ donde $e\mathscr{I}=I$. Dado que $\frac{e\bar{I}}{N(I)}\cdot\mathscr{I}=\mathcal{O}$, tenemos que $\frac{e\bar{I}}{N(I)}\subseteq\mathscr{J}$, y en consecuencia $\mathcal{O}\subseteq\mathscr{J}\mathscr{I}$. Solo queda probar que $\mathscr{J}$ es un ideal fraccionario.

Sea $\mathscr{I}=\frac{d}{e}(\mathbb{Z}a+\mathbb{Z}(-b+\delta))$, con $a,d,e,b\in\mathbb{Z}$ y $a,e,d\neq 0$. Entonces $0\neq da\in\mathscr{I}\cap\mathbb{Z}$. Por tanto $da\mathscr{I}\subseteq\mathcal{O}$. Y ademas $da\mathscr{I}$ es un ideal de $\mathcal{O}$, ya que

i) Si $x, y \in \mathscr{J}$, entonces $dax - day = da(x-y) \in da\,\mathscr{J}$ $((x-y)\mathscr{I} \subseteq x\mathscr{I} + y\mathscr{I} \subseteq \mathcal{O})$.

ii) Si $\alpha \in \mathcal{O}$ y $x \in \mathscr{J}$ entonces $\alpha dax = da\alpha x \in da\,\mathscr{J}$ $(\alpha x\mathscr{I} = x\alpha\mathscr{I} \subseteq x\mathscr{I} \subseteq \mathcal{O})$.

5. El Grupo de Clases de Ideales y la Geometría de los Números

En el siguiente capítulo se probará el segundo resultado principal del trabajo, es decir, la existencia de un grupo finito conocido como grupo de clases de ideales. Este grupo nos indicará, según su tamaño, cómo de lejos se encuentra el anillo de enteros cuadráticos de ser un dominio de factorización única. Además se han incluido numerosos ejemplos en los que se observa cómo calcular el grupo de clases de ideales de un cuerpo cuadrático.

5.1. El Grupo de Clases de Ideales

En el Capítulo anterior definimos el grupo de ideales fraccionarios $\mathbb{I}_F$, pero resulta que no es un invariante especialmente interesante de F, ya que como veremos en el Ejercicio 5.3, para cuerpos F, F' distintos, $\mathbb{I}_F \cong \mathbb{I}_{F'}$. Para conseguir un objeto que realmente refleje la aritmética de F, vamos a considerar un cociente de $\mathbb{I}_F$

Definición 5.1. Sea $\mathbb{P}_F$ el subgrupo de $\mathbb{I}_F$ formado por todos los ideales fraccionarios principales. El cociente

$$\mathrm{Cl}(F) = \mathbb{I}_F/\mathbb{P}_F$$

se denomina **grupo de clases de ideales** de F.

El grupo de clases ideales es trivial precisamente cuando todos los ideales fraccionarios en F son principales, es decir, cuando $\mathcal{O}$ es un dominio de ideales principales (PID). En los casos en que $\mathrm{Cl}(F)$ no es trivial, mide cuanto de lejos está $\mathcal{O}$ de ser un PID. El siguiente teorema, que se probará a lo largo del Capítulo, afirma que nunca está demasiado lejos.

Teorema 5.1. *Para cualquier cuerpo cuadrático F, $Cl(F)$ es finito.*

Definimos el **número de clases** de F como $h(F) = |\mathrm{Cl}(F)|$.

(a) Sean $\mathscr{I}$ y $\mathscr{J}$ ideales fraccionarios. Un elemento típico de $\mathrm{Cl}(F)$ es la clase lateral $[\mathscr{I}]=\mathbb{P}_F\mathscr{I}$, a la que llamamos clase del ideal de $\mathscr{I}$. Por la definición de grupo cociente, $[\mathscr{I}] = [\mathscr{J}]$ si y solo si $\mathscr{I} = (\mathcal{O}\alpha)\mathscr{J} = \alpha\mathscr{J}$ para cierto $\alpha \in F\backslash 0$. Dos ideales están en la misma clase precisamente cuando son proporcionales. En particular, la identidad de $\mathrm{Cl}(F)$ es $[\mathcal{O}]$, la clase de ideales fraccionarios principales.

(b) Para cualquier ideal fraccionario $\mathscr{I}$ existe un $k \in \mathbb{Z}$ tal que $I = k\mathscr{I} \subseteq \mathcal{O}$. Entonces $[\mathscr{I}]=[k\mathscr{I}] = [I]$, por tanto, toda clase de ideales está representada por un ideal integral. Podemos definir las clases de ideales sin salir de $\mathcal{O}$:$[I] = [J]$ para dos ideales I, J de $\mathcal{O}$, si y solo si existen $\beta, \gamma \in \mathcal{O}$ tales que $\gamma I = \beta J$.

(c) El inverso en $\mathrm{Cl}(F)$ se obtiene por conjugación. La identidad $I\bar{I} = \mathcal{O}\cdot \mathrm{N}I$ se traslada a $[I][\bar{I}] = [\mathcal{O}]$, o $[I]^{-1} = [\bar{I}]$.

(d) Por la Factorización Única de los Ideales, cada elemento de $\mathrm{Cl}(F)$ es un producto de clases de ideales primos. En términos de teoría de grupos, esas clases forman un conjunto de generadores del grupo $\mathrm{Cl}(F)$. Obtenemos relaciones entre ellos factorizando ideales principales.

Ejemplo 5.1. En el Ejercicio 4.5, calculamos que

$$\mathbb{Z}[\sqrt{-5}](5+\sqrt{-5}) = P_2 \cdot P_3 \cdot P_5,$$

Lo que nos da la siguiente relación en $\mathrm{Cl}(\mathbb{Q}[\sqrt{-5}])$: $[P_2][P_3][P_5] = [\mathcal{O}]$. Podemos observar que el ideal P_2 no es principal; además, la clase $[P_2]$ tiene orden 2, ya que $P_2^2 = \mathcal{O} \cdot 2$. Veremos más adelante que $\mathrm{Cl}(\mathbb{Q}[\sqrt{-5}])$ es cíclico de orden 2, generado por $[P_2]$.

Deduciremos que $\mathrm{Cl}(F)$ es finito utilizando una propiedad geométrica de los ideales, vistos como retículos en un plano.

Proposición 5.1. *Fijada una constante positiva $\mathfrak{M}_F$, cada una de estas afirmaciones implica la siguiente:*

(a) Cada ideal fraccionario $\mathscr{I}$ contiene un $\alpha \neq 0$ para el cual $|N\alpha| \leq \mathfrak{M}_F \cdot N\mathscr{I}$.

(b) Cada clase ideal de $Cl(F)$ contiene un ideal integral I de norma $NI \leq \mathfrak{M}_F$.

(c) El grupo de clases ideales de F es finito.

Demostración. Para probar que (a) implica (b), debemos encontrar en cada clase ideal $[\mathscr{J}]$ un ideal entero de norma pequeña. Para ello buscamos un $\alpha \in F \backslash 0$ tal que $I = \alpha\mathscr{J} \subseteq \mathcal{O}$ y $\mathrm{N}(\alpha\mathscr{J}) \leq \mathfrak{M}_F$, es decir

$$\alpha \in \mathscr{J}^{-1} \backslash 0 \text{ y } |\mathrm{N}\alpha| \leq \tfrac{\mathfrak{M}_F}{N\mathscr{J}}.$$

Aplicando la afirmación (a) a $\mathscr{I} = \mathscr{J}^{-1}$ conseguimos tal α.

Ahora asumamos que (b) se cumple. Para deducir (c), es suficiente con probar que hay un número finito de ideales I de $\mathcal{O}$ con norma $\mathrm{N}I \leq \mathfrak{M}_F$. Para ello, basta con probar que una vez fijado $B \in \mathbb{N}$, solo hay un número finito de ideales de norma B.

La forma estándar $I = d(\mathbb{Z}a + \mathbb{Z}(-b+\delta))$ es única si requerimos que $d > 0$ y $0 \leq b < a$. La ecuación $\mathrm{N}I = d^2a = B$ tiene un número finito de soluciones $d, a \in \mathbb{N}$ y para cada una de ellas hay un número finito de números b cumpliendo que $0 \leq b < a$ y $b^2 - tb + n \equiv 0$ (mód a).

□

La afirmación (a), y con ella el tamaño finito de $\mathrm{Cl}(F)$, se reduce a la tarea geométrica de encontrar en el retículo un punto distinto de cero cercano al origen. En la siguiente sección buscaremos una condición suficiente para la existencia de tal punto.

5.2. El Teorema de Minkowski

El hecho geométrico al que hemos hecho referencia en la subsección anterior es el Teorema de Minkowski: una región plana lo suficientemente grande, simétrica y regular contiene un punto distinto de cero del retículo.

Definición 5.2. Decimos que un conjunto $S \subseteq \mathbb{R}^2$ es **bueno** si satisface las siguientes condiciones:

(a) S posee simetría central respecto a 0: si $x \in S$, entonces $-x \in S$.

(b) S es convexo: todo segmento que una dos puntos de S está contenido en S.

(c) S es medible: tiene sentido hablar de la integral $A(S) = \iint_S dx\,dy$ que define el área de S.

No vamos a tener que preocuparnos por la condición técnica (c), ya que se cumplirá de manera obvia en todos los conjuntos S que encontremos. Denotamos el área del paralelogramo fundamental de un retículo Λ como $A(\Lambda)$.

Teorema 5.2 (Minkowski)**.** *Sean $\Lambda, S \in \mathbb{R}^2$ un retículo y una región buena respectivamente. Si $A(S) > 4A(\Lambda)$, entonces existe un punto distinto de cero en $S \cap \Lambda$. Si S es cerrado, la condición más suave $A(S) \geq 4A(\Lambda)$ es suficiente.*

La condición del área del Teorema de Minkowski es suficiente pero no necesaria. Cualquier $x \in \Lambda$ se puede unir a $-x$ mediante un rectángulo bueno de área arbitrariamente pequeña.

Demostración. Antes de empezar con la argumentación formal, veamos lo que ocurre en la Figura 3 . Los elementos de Λ son los puntos, aquellos que están en negrita pertenecen al retículo ampliado 2Λ con paralelogramo fundamental Π.

Se han nombrado de A a H las ocho traslaciones de Π que intersecan con la región buena S. Imaginemos los paralelogramos como azulejos de cristal transparente en los que S está pintada de color opaco. Si apilamos los azulejos uno encima de otro proyectaríamos las sombras que produce S sobre el paralelogramo inferior, cuya área es $A(\Pi) = 4A(\Lambda)$. El área total de las regiones pintadas suma $A(S)$. Por hipótesis, $A(S) > 4A(\Lambda)$, luego debe haber al menos dos azulejos con parte de sus sombras superpuestas. Tomamos ahora dos puntos $x, y \in S$ pertenecientes a los dos azulejos anteriores, de forma que proyectan la misma sombra. El hecho de que proyecten la misma sobra quiere decir que x e y tienen la misma posición relativa en sus respectivos azulejos. Observamos en la Figura, y vamos a probar a continuación, que $\gamma = \frac{x-y}{2}$ está contenido en $\Lambda\backslash 0$ y S como deseábamos. Formalmente,

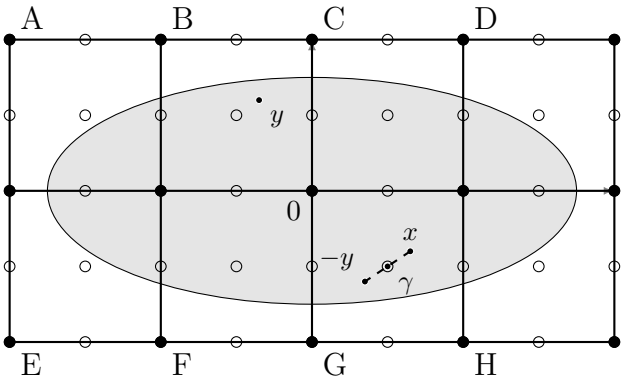

Figura 3: Una región buena S cubierta por paralelogramos.

podemos pensar que las sombras de los azulejos están proyectadas sobre el paralelogramo fundamental Π de 2Λ. Para $\alpha \in 2\Lambda$, denotamos $\Pi_\alpha = \{p + \alpha : p \in \Pi\}$ la traslación de Π por α. El conjunto $S_\alpha = (\Pi_\alpha \cap S) - \alpha \subseteq \Pi$ es la representación rigurosa de la proyección de las sombras de $\Pi_\alpha \cap S$ sobre el azulejo inferior.

Supongamos que $\alpha, \beta \in 2\Lambda$ distintos para los cuales $S_\alpha \cap S_\beta \neq 0$. Tomamos $z \in S_\alpha \cap S_\beta$. Existen puntos $x \in \pi_\alpha \cap S$ e $y \in \Pi_\beta \cap S$ tales que $z = x - \alpha = y - \beta$. Luego $\gamma = (x-y)/2 = (\alpha - \beta)/2$ pertenece a $\Lambda \backslash 0$, ya que $\alpha, \beta \in 2\Lambda$. γ es el punto medio del segmento que une x y $-y$, $-y$ pertenece a S por simetría, y por convexidad, todo el segmento está contenido en S. Por tanto, γ es un punto distinto de cero en $S \cap \Lambda$, probando el teorema en caso de que la suposición hecha al inicio del párrafo sea cierta.

Supongamos, por el contrario, que los S_α son subconjuntos disjuntos de Π. Eso justifica la primera igualdad de la cadena

$$A\left(\bigsqcup_{\alpha \in 2\Lambda} S_\alpha\right) = \sum_{\alpha \in 2\Lambda} A(S_\alpha) = A\left(\bigsqcup_{\alpha \in 2\Lambda} (\Pi_\alpha \cap S)\right) = A(S).$$

Los $\Pi_\alpha \cap S$ son siempre disjuntos, lo que junto a la invarianza del área por traslaciones explica la segunda igualdad. La tercera igualdad es cierta dado que las traslaciones de Π cubren todo el plano, en concreto todo S. Dado que todo $S_\alpha \subseteq \Pi$, deducimos que $A(S) \leq A(\Pi) = 4A(\Lambda)$, contradiciendo la hipótesis del teorema.

En el Ejercicio 5.1 se probará la condición más débil cuando S es cerrado. □

5.3. Aplicación a Ideales

Fijado un cuerpo cuadrático F, en la Proposición 5.1 vimos que podemos deducir la finitud del grupo de clases ideales $\mathrm{Cl}(F)$ a partir de la siguiente afirmación: *Existe una constante $\mathfrak{M}_F$ para la cual se cumple que: cada ideal fraccionario $\mathscr{I}$ contiene un $\alpha \neq 0$ tal que $|N\alpha| \leq \mathfrak{M}_F \cdot N\mathscr{I}$.*

El valor de $\mathfrak{M}_F$ depende únicamente del cuerpo F, no del ideal fraccionario. Para calcular de manera eficiente el orden finito de los grupos de clases ideales, vamos a utilizar la cota de la Proposición 5.1(b), por lo que queremos que $\mathfrak{M}_F$ sea lo más pequeño posible. Vamos a determinar $\mathfrak{M}_F$ de forma separada para cuerpos reales e imaginarios.

Empezaremos con F un cuerpo cuadrático imaginario. Por la Proposición 4.4, podemos pensar en cualquier ideal fraccionario $\mathscr{I}$ en F como un retículo en el plano complejo.

Proposición 5.2. *Sea $\mathscr{I}$ un ideal fraccionario en un cuerpo cuadrático imaginario F. El paralelogramo fundamental de $\mathscr{I}$ tiene área $A(\mathscr{I}) = (\sqrt{|D_F|}/2) \cdot N\mathscr{I}$.*

Demostración. Escribimos $\mathscr{I} = q(\mathbb{Z}a + \mathbb{Z}(-b+\delta))$ como en el Corolario 4.7. Su paralelogramo fundamental respecto a la base $\{qa, q(-b+\delta)\}$ tiene base $|qa|$ y altura $|q\mathrm{Im}\delta|$, por tanto, $A(\mathscr{I}) = |qa| \cdot |q\mathrm{Im}\delta| = \mathrm{N}\mathscr{I}\sqrt{|D_F|}/2$. □

Para aplicar el Teorema de Minkowski al retículo $\mathscr{I}$ y al disco cerrado S centrado en el origen, necesitamos que el disco satisfaga $A(S) \geq 4A(\mathscr{I}) = 2\sqrt{|D_F|} \cdot \mathrm{N}\mathscr{I}$. El menor de tales discos viene dado por

$$S = \{z : |z| \leq \sqrt{(2/\pi)\sqrt{|D_F|} \cdot \mathrm{N}\mathscr{I}}\}$$

El Teorema de Minkowski produce un punto $0 \neq \alpha \in S \cap \mathscr{I}$, para el cual

$$\mathrm{N}\alpha = \alpha\bar{\alpha} = |\alpha|^2 \leq \frac{2}{\pi}\sqrt{|D_F|} \cdot \mathrm{N}\mathscr{I}.$$

Es decir, $\mathfrak{M}_F = 2\sqrt{|D_F|}/\pi$. Por tanto, queda probada la finitud de $\mathrm{Cl}(F)$ cuando F es un cuerpo cuadrático imaginario.

Por contra, el anillo de enteros $\mathcal{O}$ de un cuerpo cuadrático real F es un subconjunto denso de la recta real. Para aplicar el Teorema de Minkowski a $\mathcal{O}$ y sus ideales necesitamos una forma de verlos como retículos de un plano.

Cuando pensamos en $\mathbb{Q}[\sqrt{319}]$ como un subconjunto de $\mathbb{R}$, estamos siguiendo la convención usual de cálculo $\sqrt{319} = 17{,}8605....$ Algebráicamente hablando esto es engañoso, la única propiedad de $\sqrt{319}$ que hemos utilizado es que es solución de $x^2 - 319 = 0$. Perdemos información salvo que le demos la misma importancia a ambas soluciones de la ecuación. Esto sugiere identificar $\sqrt{319}$ con el vector $(-17{,}8605..., 17{,}8605...) \in \mathbb{R}^2$, que se puede extender para un $\alpha \in \mathbb{Q}[\sqrt{319}]$ arbitrario mediante

$$\rho(\alpha) = (\bar{\alpha}, \alpha).$$

Esta fórmula define una inyección $\rho : F \hookrightarrow \mathbb{R}^2$ para cualquier cuerpo cuadrático real F. Sabemos que $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\frac{D_F + \sqrt{D_F}}{2}$. Su encaje, $\rho(\mathcal{O})$, es un retículo en $\mathbb{R}^2$ porque está generado por los vectores linealmente independientes

$$\rho(1) = (1, 1) \quad \text{y} \quad \rho(\tfrac{D_F + \sqrt{D_F}}{2}) = (\tfrac{D_F - \sqrt{D_F}}{2}, \tfrac{D_F + \sqrt{D_F}}{2}).$$

De forma similar, $\rho(\mathscr{I})$ es un retículo para cualquier ideal fraccionario $\mathscr{I}$. Satisface la siguiente Proposición análoga a 5.2.

Proposición 5.3. *Sea $\mathscr{I}$ un ideal fraccionario de un cuerpo cuadrático real F. El paralelogramo fundamental de $\rho(\mathscr{I})$ tiene área $A(\mathscr{I}) = \sqrt{D_F} \cdot N\mathscr{I}$.*

Cuando F es imaginario, la función distancia-al-origen-al-cuadrado $\mathbb{C} \to \mathbb{R}, z \mapsto |z|^2$, se limita a la norma en F. Este hecho provee la relación crucial entre la geometría del retículo $\mathscr{I}$ y la aritmética del cuerpo F. Una función análoga de $\mathbb{R}^2 \to \mathbb{R}$ en el caso real es $(x, y) \mapsto xy$, que envía $\rho(\alpha) = (\bar{\alpha}, \alpha)$ a $\bar{\alpha}\alpha = \mathrm{N}\alpha$.

Sea $\mathscr{I}$ un ideal fraccionario en un cuerpo cuadrático real F. Consideramos los subconjuntos de $\mathbb{R}^2$ representados en la Figura 4 y definidos por

$$H = \{(x, y) : |xy| \leq A(\mathscr{I})/2\}$$

$$S = \{(x, y) : |x \pm y| \leq \sqrt{2A(\mathscr{I})}\}.$$

Resulta natural considerar H, dado que queremos acotar la norma de $\alpha \in \mathscr{I}$ por un múltiplo de $A(\mathscr{I})$. Desafortunadamente, el Teorema de Minkowski no se puede aplicar al conjunto no convexo H. Las cotas en la definición de H y S han sido escogidas de forma que $A(S) = 4A(\mathscr{I})$. Aplicando el Teorema de Minkowski a S y al retículo $\rho(\mathscr{I})$ obtenemos un $\alpha \in \mathscr{I} \backslash 0$ para el cual $\rho(\alpha) = (\bar{\alpha}, \alpha) \in S \subset H$. Por definición de H,

$$|\mathrm{N}\alpha| = |\bar{\alpha}\alpha| \leq A(\mathscr{I})/2 = (\sqrt{D_F}/2) \cdot \mathrm{N}\mathscr{I}.$$

Es decir, $\mathfrak{M}_F = \sqrt{D_F}/2$, y queda probada la finitud de $\mathrm{Cl}(F)$ para cualquier cuerpo cuadrático F.

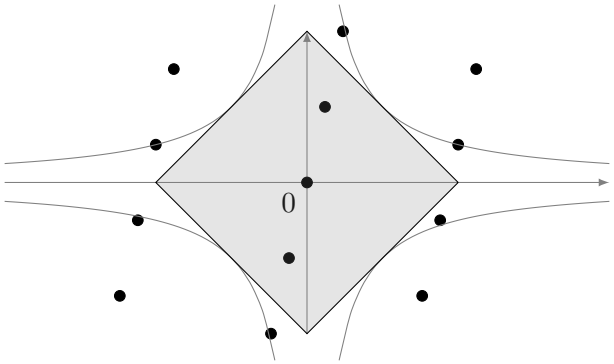

Figura 4: El cuadrado $S = \{(x, y) : |x \pm y| \leq \sqrt{2A(I)}\}$ contenido en la estrella hiperbólica $H = \{(x, y) : |xy| \leq A(I)/2\}$.

5.4. Algunos Cálculos con el Grupo de Clases Ideales

Extraemos de la sección anterior y la Proposición 5.1(b), el enunciado que nos va a permitir listar explícitamente los elementos de $\mathrm{Cl}(F)$.

Proposición 5.4 (cota de Minkowski)**.** *Cada clase ideal en $Cl(F)$ contiene un ideal de norma a lo sumo $\mathfrak{M}_F$, con*

$$\mathfrak{M}_F = \sqrt{|D_F|} \cdot \begin{cases} \frac{2}{\pi} & \text{para } F \text{ imaginario} \\ \frac{1}{2} & \text{para } F \text{ real.} \end{cases}$$

Para entender como utilizar esta proposición para calcular grupos de clases ideales, empezamos con unos ejemplos sencillos.

Ejemplo 5.2. Sea $F = \mathbb{Q}[i]$, $\mathcal{O} = \mathbb{Z}[i]$. La cota de Minkowski nos permite representar cualquier clase ideal mediante un ideal I cumpliendo que

$$\mathrm{N}I \leq \mathfrak{M}_F = \frac{2}{\pi}\sqrt{|-4|} \approx 1{,}27.$$

Como $\mathrm{N}I \in \mathbb{N}$, tenemos que $\mathrm{N}I = 1$, luego $I = \mathcal{O}$. Así, cada clase contiene a $\mathcal{O}$, luego $\mathrm{Cl}(F) = \{[\mathcal{O}]\}$, y $\mathbb{Z}[i]$ es un DIP. Conocíamos esto desde el Capítulo 1, la cuestión es que ahora podemos probarlo sin necesidad del algoritmo de la división en $\mathbb{Z}[i]$.

Ejemplo 5.3. Sea $F = \mathbb{Q}[\sqrt{-19}]$, luego $\mathcal{O} = \mathbb{Z}[(1 + \sqrt{-19}/2)]$. Vamos a ver que $\mathcal{O}$ es un PID, a pesar de no ser un Dominio Euclídeo por el Ejercicio 2.2. La cota de Minkowski nos garantiza que cada clase ideal contiene un representante I con

$$\mathrm{N}I \leq \mathfrak{M}_F = \frac{2}{\pi}\sqrt{19} \approx 2{,}7.$$

Si $\mathrm{N}I = 1$, entonces $I = \mathcal{O}$, y $[I]$ es la identidad en $\mathrm{Cl}(F)$. Si $\mathrm{N}I = 2$, entonces I es factor de 2. Esto es imposible, ya que 2 es inerte en $\mathbb{Q}[\sqrt{-19}]$, y el único ideal primo que lo divide, es decir, el propio $\mathcal{O} \cdot 2$, tiene norma 4. Concluimos que $h(F) = 1$.

Ejemplo 5.4. Sea $F = \mathbb{Q}[\sqrt{-5}]$, luego $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$ y $D_F = -20$. Sea $P_2 = \mathbb{Z}\cdot 2 + \mathbb{Z}(1+\sqrt{-5})$ el único ideal de norma 2. Vimos en el Ejemplo 5.1 que $\mathrm{Cl}(F)$ tiene al menos dos elementos, $[\mathcal{O}]$ y $[P_2]$. No hay ninguno más: la cota de Minkowski muestra que toda clase ideal distinta de la identidad contiene un ideal I con

$$2 \leq \mathrm{N}I \leq \frac{2}{\pi}\sqrt{20} \approx 2{,}8$$

por lo que $\mathrm{N}I = 2$ e $I = P_2$. Así, $\mathrm{Cl}(F)$ es cíclico de orden 2, generado por $[P_2]$.

Ejemplo 5.5. Sea $F = \mathbb{Q}[\sqrt{15}]$, luego $\mathcal{O} = \mathbb{Z}[\sqrt{15}]$ y $D_F = 60$. Por la cota de Minkowski, todas las clases ideales salvo $[\mathcal{O}]$ contienen un ideal I, cuya norma está acotada por

$$2 \leq \mathrm{N}I \leq \frac{1}{2}\sqrt{60} \approx 3{,}9,$$

es decir, $\mathrm{N}I = 2$ o 3. Existe un único ideal de cada norma, dado que 2 y 3 dividen a D_F y por tanto son ramificados, aplicando el Teorema 4.4:

$$\mathcal{O}\cdot 2 = P_2^2 \quad \textit{donde} \quad P_2 = \mathbb{Z}\cdot 2 + \mathbb{Z}(1+\sqrt{15}) \tag{1}$$

$$\mathcal{O}\cdot 3 = P_3^2 \quad \textit{donde} \quad P_2 = \mathbb{Z}\cdot 3 + \mathbb{Z}(\sqrt{15}) \tag{2}$$

Luego $\mathrm{Cl}(F)$ tiene a la sumo tres elementos, $[\mathcal{O}], [P_2], [P_3]$, teniendo en cuenta que algunas de las clases anteriores podrían coincidir. Dado que $\mathcal{O}\cdot 2 = P_2^2$, tenemos que $[P_2]$ es trivial o tiene orden 2. Lo mismo ocurre para $[P_3]$. Para poder discernir en estos casos, utilizaremos el siguiente lema.

Lema 5.1. *Sea F un cuerpo cuadrático con anillo de enteros $\mathcal{O}$. Sea P un ideal de $\mathcal{O}$ con norma prima. Entonces P es principal si y solo si existe un $\alpha \in \mathcal{O}$ tal que $\mathrm{N}\alpha = \pm NP$.*

La demostración del Lema anterior se hará en el Ejercicio 5.1.

Para aplicar el Lema a P_2 y P_3, buscamos soluciones en $\mathbb{Z}$ de $\mathrm{N}(x+y\sqrt{15}) = x^2 - 15y^2 = \pm 2$ o ± 3. Reduciendo estas ecuaciones en módulo 5, tenemos que $x^2 \equiv \pm 2 \pmod 5$, que no tiene solución, ya que $\left(\frac{\pm 2}{5}\right) = -1$. Concluimos por tanto que $[P_2] \neq [\mathcal{O}] \neq [P_3]$, luego tanto $[P_2]$ como $[P_3]$ tienen orden 2, y $\mathrm{Cl}(F)$ tiene 2 o 3 elementos. Como $\mathbb{Z}/3\mathbb{Z}$ no tiene ningún elemento de orden 2, $\mathrm{Cl}(F)$ no puede tener tres elementos. Concluimos que $\mathrm{Cl}(F) \cong \mathbb{Z}/2\mathbb{Z}$ y $[P_2] = [P_3]$.

La identidad $[P_2][P_3]^{-1} = [\mathcal{O}]$ es un ejemplo de una relación en $\mathrm{Cl}(F)$. Podemos probarla directamente observando que $\mathrm{N}(3+\sqrt{15}) = -6$. En vista de la ecuación (1), esto significa que $\mathcal{O}(3+\sqrt{15}) = P_2P_3$.

Para discriminantes más grandes, es útil sistematizar el procedimiento para calcular el grupo de clases ideales. La siguiente Proposición es una combinación directa de los dos Teoremas principales del trabajo, a saber, la factorización única de ideales (el Teorema 4.3) y la finitud del grupo de clases ideales (el Teorema 5.1).

Proposición 5.5. *El grupo de clases ideales de F está generado por un número finito de clases $[P]$, donde P abarca los ideales de norma prima acotada por $NP \leq \mathfrak{M}_F$.*

Ejemplo 5.6. Sea $F = \mathbb{Q}[\sqrt{130}]$, con $\mathcal{O} = \mathbb{Z}[\sqrt{130}]$ y $D_F = 520$. Por la Proposición anterior, un conjunto de generadores de $\mathrm{Cl}(F)$ viene dado por todos los ideales P de norma prima p satisfaciendo

$$p \leq \frac{1}{2}\sqrt{520} \approx 11{,}4$$

Los posibles p vienen dados en la siguiente tabla

p	2	3	5	7	11
$(\frac{130}{p})$	0	1	0	1	1
b	0	1	0	2	3

Aquí b define el ideal $P_p = \mathbb{Z}p + \mathbb{Z}(-b + \sqrt{130})$ (como en el Teorema 4.4) para el cual $\mathcal{O}p = P_p\bar{P}_p$. Las clases de ideales primos ramificados tienen a lo sumo orden 2: $P_2^2 = \mathcal{O} \cdot 2$, luego $[P_2]^2 = [\mathcal{O}]$, y lo mismo ocurre para $[P_5]^2 = [\mathcal{O}]$. Para encontrar otras relaciones entre los cinco generadores, factorizamos unos pocos elementos de $\mathcal{O}$, cuya norma tiene únicamente factores primos ≤ 11:

$$\mathrm{N}(12 + \sqrt{130}) = 2 \cdot 7 \qquad \mathcal{O}(12 + \sqrt{130}) = P_2P_7$$

$$\mathrm{N}(35 + 3\sqrt{130}) = 5 \cdot 11 \qquad \mathcal{O}(35 + 3\sqrt{130}) = P_5P_{11}$$

$$\mathrm{N}(10 + \sqrt{130}) = -2 \cdot 3 \cdot 5 \qquad \mathcal{O}(10 + \sqrt{130}) = P_2\bar{P}_3P_5$$

De la primera ecuación obtenemos que $[\mathcal{O}] = [P_2][P_7]$, luego $[P_7] = [P_2]$. De forma similar, $[P_5] = [P_{11}]$ y $[P_3] = [P_2][P_5]$. Así, $\mathrm{Cl}(F)$ está generado por las clases $[P_2]$ y $[P_5]$, ambas de a lo sumo orden 2. Salvo que que existan otras relaciones entre ellas, tendremos que $\mathrm{Cl}(F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Para probarlo, es suficiente mostrar que ninguna de las clases $[P_2], [P_5], [P_2][P_5] = [P_3]$ son iguales a $[\mathcal{O}]$. El Lema 5.1 reduce esta cuestión a comprobar que ninguna de las ecuaciones $x^2 - 130y^2 = \pm 2, \pm 3$ o ± 5 tiene soluciones enteras.

$x^2 - 130y^2 = \pm 5$: Reduciendo en módulo 13, tenemos que $x^2 \equiv \pm 5 \pmod{13}$, lo que es imposible, dado que $(\frac{\pm 5}{13}) = -1$. El mismo argumento muestra que $x^2 - 130y^2 = \pm 2$ no tiene soluciones, luego ambos generadores son no-triviales.

$x^2 - 130y^2 = \pm 3$: Reduciendo en módulo 5, tenemos que $x^2 \equiv \pm 3 \pmod{5}$, lo que es imposible.

Ejemplo 5.7. Sea $F = \mathbb{Q}[\sqrt{-47}]$, luego $\mathcal{O} = \mathbb{Z}[\delta]$ con $\delta^2 - \delta + 12 = 0$. Por la Proposición 5.5, $\mathrm{Cl}(F)$ está generado por ideales P de norma prima acotada por

$$\mathrm{N}P \leq \frac{2}{\pi}\sqrt{47} \approx 4{,}36$$

Factorizamos los dos posibles valores de $\mathrm{N}P$:

$$\mathcal{O} \cdot 2 = P_2\bar{P}_2 \qquad P_2 = \mathbb{Z} \cdot 2 + \mathbb{Z}\delta$$

$$\mathcal{O} \cdot 3 = P_3\bar{P}_3 \qquad P_3 = \mathbb{Z} \cdot 3 + \mathbb{Z}(-1 + \delta).$$

Cualquier relación entre $[P_2]$ y $[P_3]$ será de la forma $[P_2]^a[P_3]^b = [\mathcal{O}]$. Esto significa que $P_2^a P_3^b = \mathcal{O}\alpha$ para un cierto $\alpha \in \mathcal{O}$ de norma $2^a 3^b$. Rápidamente encontramos tal α: $\mathrm{N}\delta = 12 = 2^2 \cdot 3$. Una comprobación rápida como la del Ejercicio 4.5 muestra que

$$\mathcal{O}\delta = P_2^2 \bar{P}_3,$$

luego en $\mathrm{Cl}(F)$, $[P_3] = [P_2]^2$, es decir, podemos sustituir toda potencia de $[P_3]$ por un de $[P_2]$ y concluir que $\mathrm{Cl}(F) = \langle [P_2] \rangle$. Todo lo que queda es determinar el orden de $[P_2]$, es decir, el menor $e > 0$ para el cual existe un $\beta = x + y\delta \in \mathcal{O}$ con $P_2^e = \mathcal{O}\beta$. Tomando la norma, tenemos que

$$2^e = \mathrm{N}(x + y\delta) = x^2 + xy + 12y^2 = \left(x + \frac{y}{2}\right)^2 + \frac{47}{4}y^2.$$

Si $y = 0$ entonces $\beta = \pm 2^{e/2}$, luego $\mathcal{O}\beta = \mathcal{O} \cdot 2^{e/2} = P_2^{e/2} \bar{P}_2^{e/2}$. Esta factorización prima de $\mathcal{O}\beta$ contradice que $\mathcal{O}\beta = P_2^e$. Si $y \neq 0$, observamos que $\mathrm{N}\beta \geq \lceil 47/4 \rceil = 12$, luego $\mathrm{N}\beta$ no puede ser ni 2,ni 4 ni 8. $\mathrm{N}\beta \neq 2$ implica que P_2 no es principal.

Si $\mathrm{N}\beta = 16$, tenemos que $y = \pm 1$, de otra forma la parte derecha de la ecuación anterior es demasiado grande. Pero $x^2 + x + 12 = 16$ no tiene soluciones en $\mathbb{Z}$, lo que impide que $\mathrm{N}\beta = 16$.

Intentemos resolver $32 = x^2 + xy + 12y^2$. Como antes, no puede ser que $|y| > 1$, lo que nos lleva a una solución $(x, y) = (4, 1)$, y la factorización $\mathcal{O}(4 + \delta) = P_2^5$. Así, $\mathrm{Cl}(F) \cong \mathbb{Z}/5\mathbb{Z}$.

La conclusión del Ejemplo anterior es que, para F imaginario, resolver la ecuación $\mathrm{N}(x + y\delta) = (x - \frac{t}{2}y)^2 - \frac{D_F}{4}y^2 = n$ es fácil. Dado que $D_F < 0$, la norma crece con x e y, y solo tenemos que comprobar un número finito de valores.

Ejemplo 5.8. Para un cuerpo cuadrático real la situación es más difícil, como vamos a ver en el ejemplo de $F = \mathbb{Q}[\sqrt{223}]$. Tenemos que $\mathcal{O} = \mathbb{Z}[\sqrt{223}]$ y $D_F = 892$. Empezamos fatorizando los ideales $\mathcal{O}p$ para todos los primos p acotados por

$$p \leq \frac{1}{2}\sqrt{892} \approx 14{,}933$$

Hacemos una tabla

p	2	3	5	7	11	13
$(\frac{223}{p})$	1	1	-1	-1	1	-1
b	1	1	-	-	5	-

Los b correspondientes a $p = 2, 3, 11$ definen el ideal primo $P_p = \mathbb{Z}p + \mathbb{Z}(b + \sqrt{223})$ para el cual $\mathcal{O}p = P_p \bar{P}_p$. Hemos descartado 5,7 y 13 ya que son inertes, y por tanto pertenecen a $[\mathcal{O}]$. También ignoramos $[P_2]$, que es principal por el Lema 5.1, ya que $\mathrm{N}(15 + \sqrt{223}) = 15^2 - 223 = 2$.

Para encontrar una relación entre $[P_3]$ y $[P_{11}]$, buscamos elementos de norma pequeña divisible por 3 y por 11.

$$\mathrm{N}(16 + \sqrt{223}) = 3 \cdot 11 \qquad \mathcal{O}(16 + \sqrt{223}) = P_3 P_{11}$$

$$\mathrm{N}(14 + \sqrt{223}) = -3^3 \qquad \mathcal{O}(14 + \sqrt{223}) = P_3^3$$

Concluimos que $\mathrm{Cl}(F) = \langle [P_3] \rangle$ es isomorfo a $\mathbb{Z}/3\mathbb{Z}$, una vez que veamos que $[P_3]$ no es principal. Al igual que antes, para ello tenemos que probar que $x^2 - 223y^2 = \pm 3$ no tiene soluciones en $\mathbb{Z}$. En este caso no podemos hacerlo reduciendo en módulo primo, ya que la ecuación $x^2 - 223y^2 \equiv \pm 3 \pmod{p}$ tiene solución para cada $p \in \mathbb{N}$. Para verlo, consideremos varios casos.

Si existe un $a \in \mathbb{Z}$ con $a^2 \equiv \pm 3 \pmod{p}$, entonces $a^2 - 223 \cdot 0^2 \equiv \pm 3 \pmod{p}$. Asumamos que ni 3 ni -3 son cuadrados en módulo p. Si 223 es un cuadrado en módulo p, existe un $b \in \mathbb{Z}$ con $b^2 \equiv 4/223 \pmod{p}$. Entonces $1^2 - 223b^2 \equiv -3 \pmod{p}$. De lo contrario, ni 3 ni 223 son cuadrados, y existe un $b \in \mathbb{Z}$ cumpliendo que $b^2 \equiv 3/223 \pmod{p}$, luego $0^2 - 223b^2 \equiv -3 \pmod{p}$.

Para ver que $x^2 - 223y^2 = \pm 3$ no tiene soluciones enteras necesitaremos otras técnicas.

Podemos extraer de estos ejemplos un modelo para encontrar el grupo de clases ideales de un cuerpo cuadrático F:

(a) Calcular la cota de Minkowski $B = \lfloor \mathfrak{M}_F \rfloor$, y buscar las factorizaciones primas $\mathcal{O}p = P_p \bar{P}_p$ para todos los primos no inertes $p \leq B$. Los ideales primos P_p forma una lista de generadores de $\mathrm{Cl}(F)$, posiblemente redundantes.

(b) Buscar varios $\alpha \in \mathcal{O}$ con $\mathrm{N}\alpha$ pequeña y divisible solo por primos $\leq B$. La factorización de $\mathcal{O}\alpha$ nos dará una relación entre los generadores obtenidos en (a).

(c) Usar estas relaciones para reducir el número de generadores necesarios, hasta determinar la estructura de grupo de $\mathrm{Cl}(F)$.

Este modelo puede ser mejorado y convertido en algoritmos rápidos, implementados en diversos softwares de teoría de números. El modelo aquí planteado, a pesar de no ser el más eficaz, es suficiente para hacernos una idea de los cálculos de clases ideales.

5.5. Ejercicios

Ejercicio 5.1. *Prueba la última afirmación del Teorema de Minkowski: si la región S es cerrada, la condición más débil $A(S) \geq 4A(\Lambda)$ es suficiente para que el Teorema se cumpla.*

Vamos a probar que la suposición de que existen $\alpha, \beta \in 2\Lambda$ distintos para los cuales $S_\alpha \cap S_\beta \neq 0$ se sigue cumpliendo, y por tanto la demostración del Teorema se realiza de la misma forma. Procederemos por reducción al absurdo. Supongamos que $A(S) = 4A(\Lambda)$ y que los S_α son disjuntos.

Dado que $S_\alpha = (\Pi_\alpha \cap S) - \alpha \subseteq \Pi$, tenemos que es la intersección de Π con un conjunto cerrado (una traslación de S, que es cerrado), por tanto, con la topología inducida por $\mathbb{R}^2$ en Π, tenemos que S_α es un cerrado en Π, ya que es la intersección de un cerrado en $\mathbb{R}^2$ y Π. Como los distintos S_α son cerrados en Π y disjuntos, su unión no es conexa (la unión de cerrados disjuntos no es conexa). Luego existe un $w \in \Pi \setminus \bigsqcup_{\alpha \in 2\Lambda} S_\alpha$.

Sea $\bar{S_\alpha}$ la clausura de S_α en $\mathbb{R}^2$, que consiste en S_α y la porción adyacente de la frontera de $\overline{\Pi}$. Consideremos la función distancia $d_w : \cup \bar{S_\alpha} \to \mathbb{R}, d_w(x) = |x - w|$, está función debe tener un valor mínimo $r \neq 0$, ya que en caso de no tenerlo, debería existir una sucesión de elementos de $\cup \bar{S_\alpha}$ que tendiera a w, pero $\cup \bar{S_\alpha}$ es un conjunto cerrado, y $w \notin \cup \bar{S_\alpha}$, luego es imposible que tal sucesión exista. Por tanto, existe un disco D de radio $k < r$ de forma que $D \subset \Pi \setminus \bigsqcup_{\alpha \in 2\Lambda} S_\alpha$, lo que es una contradicción con $A(S) = A(\Pi)$.

Ejercicio 5.2. *Prueba el Lema 5.1.*

Veamos primero la implicación a derecha. Supongamos que $P = \mathcal{O}\alpha$ es un ideal principal, entonces, por el Ejercicio 4.1, $|\mathrm{N}P| = |\mathrm{N}\alpha|$.

Veamos ahora la implicación a izquierda. Supongamos que existe un $\alpha \in F$ tal que $\mathrm{N}\alpha = \mathrm{N}P$. Como $\mathrm{N}(P) = p$ primo, entonces P es un ideal primo (ya que si $P = Q_1 Q_2 \cdots Q_r$, entonces $\mathrm{N}(P) = p = \mathrm{N}(Q_1) \cdots \mathrm{N}(Q_r)$, lo que es una contradicción). Por tanto, $\mathcal{O}p = P^2$ o $\mathcal{O}p = P\bar{P}$. Ahora, $\mathcal{O}p = \mathcal{O}\mathrm{N}(P) = \mathcal{O}\mathrm{N}(\alpha) = \mathcal{O}\alpha\mathcal{O}\bar{\alpha}$. Luego por la factorización única de ideales, $\mathcal{O}\alpha = P$.

Ejercicio 5.3. *Prueba que para dos cuerpos cuadráticos diferentes F, F', se tiene que $\mathbb{I}_F \cong \mathbb{I}_{F'}$.*

Debido a la factorización única de ideales, cualquier ideal $I \subseteq \mathcal{O}$ distinto de cero se puede escribir como un producto de todos los ideales primos distintos de cero:

$$I = \prod_P P^{e_P}.$$

Donde $e_P \in \mathbb{Z}_{\geq 0}$, y $e_P = 0$ salvo un número finito de ideales primos P. Para $I = \mathcal{O}$ ponemos $e_P = 0$ para todo P. Sea

$$\mathfrak{J} = \{(e_P) : e_P \in \mathbb{Z}_{\geq 0}, e_P = 0 \text{ salvo un número finito de ideales primos P}\}$$

el conjunto de las sucesiones infinitas con entradas en $\mathbb{Z}_{\geq 0}$ y solo un número finito de entradas distintas de 0. Se tiene que este conjunto forma un grupo bajo la suma componente a componente.

Veamos que la asignación $I \mapsto (e_P)$ se extiende a un isomorfismo de grupos $\mathbb{I}_F \cong \mathfrak{J}$. En primer lugar, veamos que es un homomorfismo de grupos. Sean $I = P_1^{e_{P_1}} P_2^{e_{P_2}} \cdots P_r^{e_{P_r}}$ y $J = P_1^{e'_{P_1}} P_2^{e'_{P_2}} \cdots P_r^{e'_{P_r}}$ la factorización prima de dos ideales, con $e_P, e'_P \in \mathbb{Z}_{\geq 0}$ y eligiendo r de forma que sus sucesiones asociadas, $(e_P), (e'_P)$ no tengan ningún valor distinto de 0 a partir de la componente r. Entonces $IJ = P_1^{e_{P_1}+e'_{P_1}} P_2^{e_{P_2}+e'_{P_2}} \cdots P_r^{e_{P_r}+e'_{P_r}}$, por tanto, la sucesión asociada a IJ es $(e_P) + (e'_P)$.

Veamos que la asignación es inyectiva. Sean I, J dos ideales con la misma sucesión asociada $(e_P) = (e_{P_1}, \ldots, e_{P_r}, 0, \ldots)$, de tal forma que a partir de la componente r la sucesión solo tiene ceros, entonces tenemos que $I = P_1^{e_{P_1}} P_2^{e_{P_2}} \cdots P_r^{e_{P_r}} = J$.

Veamos que es suprayectiva. Sea $(e_P) = (e_{P_1}, \ldots, e_{P_n}, 0, \ldots)$ una sucesión de $\mathfrak{J}$, de forma que todas las componentes a partir de la componente n son ceros. Entonces tenemos que el ideal $I = P_1^{e_{P_1}} P_2^{e_{P_2}} \cdots P_n^{e_{P_n}}$ tiene asociada esa sucesión, luego la asignación es suprayectiva.

Así, podemos concluir que, para cualquier cuerpo cuadrático F, se tiene que $\mathbb{I}_F \cong \mathfrak{J}$.

Apéndice: Formas cuadráticas

En esta sección volvemos a las raíces de la teoría de números algebraica de finales del siglo XVIII. Sus padres, Lagrange, Legendre y Gauss no poseían las herramientas algebraicas que hemos utilizado durante el trabajo. Descubrieron el grupo de clases de ideales trabajando con ciertas funciones sobre el retículo estándar $\Lambda_0 = \{\begin{bmatrix} x \\ y \end{bmatrix} : x, y \in \mathbb{Z}\}$ conocidas como formas.

El estudio de las formas, sus relaciones con los ideales de $\mathcal{O}$ y sus aplicaciones al cálculo del grupo de clases de ideales, realizado de manera rigurosa y pormenorizada, daría pie a otro Trabajo de Fin de Grado en sí mismo. Por lo tanto, puesto que no contamos con el espacio suficiente para llevar a cabo tal estudio, nos limitaremos a dar una serie de pinceladas acerca de la teoría y algunos ejemplos. Con ello se pretende que podamos obtener una idea intuitiva acerca de este tema.

Definición 5.3. Una **forma** es una función $q : \Lambda_0 \to \mathbb{Z}$ dada por $q(x, y) = ax^2 + bxy + cy^2$ para ciertos $a, b, c \in \mathbb{Z}$.

Definición 5.4. Sea $\mathscr{I} = \mathbb{Z}\alpha + \mathbb{Z}\beta$ un ideal fraccionario de un cuerpo cuadrático F, la expresión

$$q_{\mathscr{I},\alpha,\beta}(x, y) = \frac{\mathrm{N}(x\alpha - y\beta)}{\mathrm{N}\mathscr{I}} = \frac{\mathrm{N}\alpha}{\mathrm{N}\mathscr{I}}x^2 - \frac{\mathrm{Tr}(\bar{\alpha}\beta)}{\mathrm{N}\mathscr{I}}xy + \frac{\mathrm{N}\beta}{\mathrm{N}\mathscr{I}}y^2$$

tiene coeficientes en $\mathbb{Z}$ y por tanto define una forma, que se conoce como **forma asociada** a $(\mathscr{I}, \alpha, \beta)$. Esta forma es invariante si la escalamos por productos de elementos de $F^\times$:

$$q_{\gamma\mathscr{I},\gamma\alpha,\gamma\beta}(x, y) = q_{\mathscr{I},\alpha,\beta}(x, y), \text{ cuando } \mathrm{N}\gamma > 0.$$

Esto sugiere una conexión entre formas y clases ideales.

Dos formas asociadas son **equivalentes** si podemos obtener una a partir de la otra mediante un cambio lineal de variables dado por $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z})$. Decimos que son **propiamente equivalentes** si $\det\begin{bmatrix} a & b \\ c & d \end{bmatrix} = 1$.

Proposición 5.6. *Para cualquier forma, existe una secuencia de cambios de variables lineales que produce una forma $ax^2 + bxy + cy^2$ cumpliendo que*

$$|b| \leq |a| \leq |c|, \text{ y } b \geq 0 \text{ cuando } |a| = |b| \text{ o } |a| = |c|.$$

Le debemos al propio Legendre un algoritmo para realizar estos cambios de variable.

Definición 5.5. Una forma es **descomponible** si es un producto de dos polinomios lineales con coeficientes en $\mathbb{Q}$: $q(x, y) = a(x - ry)(x - sy)$ para $a \in \mathbb{Z}$ y $r, s \in \mathbb{Q}$. De lo contrario, la forma es **indescomponible**.

Definición 5.6. Una forma q tiene asociados dos invariantes con valores en $\mathbb{Z}$:

(a) El **contenido**, cont q =m.c.d.(a, b, c). Si cont $q = 1$, decimos que la forma es **primitiva**.

(b) El **discriminante**, disc $q = b^2 - 4ac$.

Definición 5.7. Una **forma cuadrática** es una forma primitiva indescomponible.

Una forma es descomponible precisamente cuando su discriminate es un cuadrado perfecto.

Definición 5.8. Sean $\mathcal{Q}$ el conjunto de todas las formas cuadráticas y $\mathcal{H}$ el de todos los números cuadráticos. La función **parámetro** $\iota_{\mathcal{Q}\mathcal{H}}$: $\mathcal{Q} \to \mathcal{H}$ viene dada por

$$q(x,y) = ax^2 + bxy + cy^2 \mapsto \eta_q = \frac{-b + \sqrt{\text{disc } q}}{2a}$$

Definición 5.9. Sea F un cuerpo cuadrático.

(a) Un ideal principal es **totalmente positivo** si es de la forma $\mathcal{O}\alpha$ con $\text{N}\alpha > 0$. Tales ideales forman un subgrupo $\mathbb{P}_F^+ \subseteq \mathbb{P}_F \subseteq \mathbb{I}_F$.

(b) El **grupo de clases estrictas de ideales** de F es el grupo cociente $\text{Cl}^+(F) = \mathbb{I}_F/\mathbb{P}_F^+$.

(c) El **número de clases estrictas de ideales** de F es $h^+(F) = |\text{Cl}^+(F)|$.

El grupo de clases ideales fino es claramente una variación del grupo de clases ideales. Es "estricto" porque tomamos el cociente por un subgrupo más pequeño. Está implícito en la definición de $h^+(F)$ el hecho de que $\text{Cl}^+(F)$ es finito. Para F imaginario es obvio, ya que $\mathbb{P}_F^+ = \mathbb{P}_F$, y por tanto $\text{Cl}^+(F)$ =Cl(F). En el caso real, tomando el homomorfismo de grupos suprayectivo ψ :Cl$^+(F) \to$ Cl(F) dado por

$$\psi(\mathbb{P}_F^+ \cdot \mathscr{I}) = \mathbb{P}_F \cdot \mathscr{I}.$$

Este homomorfismo es un isomorfismo salvo que la unidad fundamental de F cumpla que $\text{N}\epsilon_F = 1$. En ese caso kerψ es cíclico de orden 2, generado por la clase lateral $\mathbb{P}_F^+ \cdot (\mathcal{O}\sqrt{D})$, y por tanto el tamaño de $\text{Cl}^+(F)$ es el doble del de Cl(F).

Tenemos ya definidos los elementos suficientes para poder enunciar el Teorema principal respecto a las formas. Dado que como se ha comentado al inicio de este Capítulo, no contamos con el espacio suficiente para desarrollar la teoría necesaria para demostrarlo, vamos a realizar un ejemplo ilustrativo que nos permita tener un idea intuitiva.

Ejemplo 5.9. Vamos a buscar todas las formas $ax^2+bxy+cy^2$ con discriminante $b^2-4ac = -47$, $a > 0$ (y por tanto $c > 0$) y satisfaciendo la condición de la Proposición anterior, es decir $|b| \leq a \leq c$ y $b \geq 0$ cuando $a = |b|$ o $a = c$. Una forma de este tipo se conoce como **forma reducida**. A partir de

$$47 = 4ac - b^2 \geq 4|b|^2 - b^2 = 3b^2$$

deducimos que $|b| < \sqrt{47/3}$ y por tanto $|b| \leq 3$. Para cada b buscamos los posibles valores de a y c factorizando $b^2 + 47 = 4ac$. Esta igualdad fuerza a que b se impar.

No hay formas reducidas con $b = \pm 3$, por que se cumpliría que $ac = 14$ y $3 \leq a \leq c$, lo que es imposible. Si $b = \pm 1$, entonces $ac = 12$ y tenemos las siguientes posibilidades:

(a) $a = 1, c = 12$: obtenemos una única forma $x^2 + xy + 12y^2$. Descartamos $x^2 - xy + 12y^2$ ya que $|b| = a$ en este caso.

(b) $a = 2, c = 6$: obtenemos dos formas, $2x^2 \pm xy + 6y^2$.

(c) $a = 3, c = 4$: volvemos a obtener dos formas, $3x^3 \pm xy + 4y^2$.

Se puede comprobar que ninguna de estas formas es propiamente equivalente.

Hay cinco formas reducidas de discriminante -47, al igual que hay cinco clases ideales en $\mathrm{Cl}(\mathbb{Q}[\sqrt{-47}]) = \langle [P_2] \rangle$, como calculamos en el Ejemplo 5.7. La invarianza cuando multiplicamos por un escalar $\gamma \in F^\times$ con $\mathrm{N}\gamma > 0$ sugiere que no es una coincidencia. En la siguiente tabla, el ideal I_k y su base están elegidos para que su forma asociada q_k sea reducida. Además, I_k está en la clase ideal $[P_2]^k$. En la tercera columna están los η_k, soluciones de $q_k(x, 1) = 0$ con parte imaginaria positiva. Los η_k están dibujados en la figura.

k	$I_k = \mathbb{Z}\alpha + \mathbb{Z}\beta$	$q_k = q_{I_k,\alpha,\beta}$	η_k
0	$\mathbb{Z} + \mathbb{Z}(-\bar{\delta})$	$x^2 + xy + 12y^2$	$\frac{-1+\sqrt{-47}}{2}$
1	$\mathbb{Z} \cdot 2 + \mathbb{Z}\delta$	$2x^2 - xy + 6y^2$	$\frac{1+\sqrt{-47}}{4}$
2	$\mathbb{Z} \cdot 3 + \mathbb{Z}(-\bar{\delta})$	$3x^2 + xy + 4y^2$	$\frac{-1+\sqrt{-47}}{6}$
3	$\mathbb{Z} \cdot 3 + \mathbb{Z}\delta$	$3x^2 - xy + 4y^2$	$\frac{1+\sqrt{-47}}{6}$
4	$\mathbb{Z} \cdot 2 + \mathbb{Z}(-\bar{\delta})$	$2x^2 + xy + 6y^2$	$\frac{-1+\sqrt{-47}}{4}$

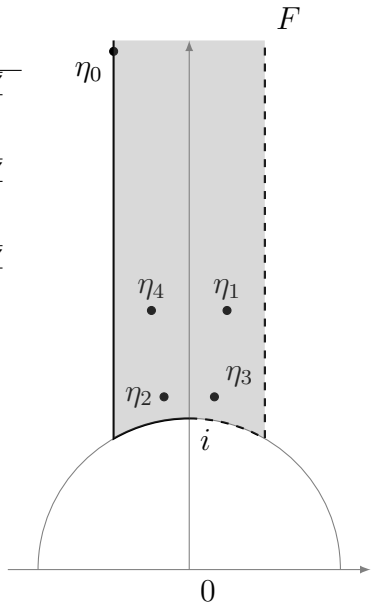

Figura 5: Formas reducidas de discriminate -47.

La tabla nos da biyecciones entre los tres conjuntos siguientes:

(a) El grupo de clases ideales $\mathrm{Cl}(\mathbb{Q}[\sqrt{-47}])$.

(b) Clases de equivalencia de las formas propiamente equivalentes, para las cuales las formas reducidas son representantes convenientes.

(c) Números cuadráticos de la forma $(-b + \sqrt{-47})/2a$ contenidos en el región sombreada F. El interior de F es $\{z \in \mathbb{C} : \mathrm{Im}z > 0, |\mathrm{Re}z| < 1/2, |z| > 1\}$.

Estas biyecciones son un ejemplo del principal resultado sobre formas, el Teorema 5.3. La correspondencia entre (a) y (b) nos ofrece una forma rápida de calcular el número de clases $h(f)$ usando simples manipulaciones con enteros. La biyección entre (b) y (c) asocia a cada forma una especio de "número de identificación", o parámetro en el plano complejo. Geométricamente, las formas reducidas son precisamente aquellas cuyo parámetro se encuentra dentro de F.

Teorema 5.3. *Sea SL_2 el grupo de las matrices de orden 2 con determinante 1, tenemos que existen las siguientes biyecciones*

$$\mathrm{Cl}^+(F) \cong \mathcal{Q}_F/\ \mathrm{SL}_2(\mathbb{Z}) \cong \mathcal{H}_F/\ \mathrm{SL}_2.$$

El Teorema anterior nos ofrece un resultado matemático de gran belleza. Nos permite estudiar el mismo objeto desde tres puntos de vista:

(a) Como $\mathcal{Q}_F/\ \mathrm{SL}_2(\mathbb{Z})$ está identificado con $\mathrm{Cl}^+(F)$, también debe tener estructura de grupo. No es para nada obvio encontrar la forma de "componer" dos clases de formas cuadráticas. Legendre estuvo cerca de dar con ella un siglo antes de que se definiera el grupo de clases de ideales, pero falló al considerar $\mathrm{GL}_2(\mathbb{Z})$ en vez de $\mathrm{SL}_2(\mathbb{Z})$ a la hora de construir la clase de equivalencia. Fue Gauss quien se dio cuenta de la importancia de $\mathrm{SL}_2(\mathbb{Z})$. Este tema tiene un sorprendente vigor en el siglo XXI, con Bhargava abriendo un importante nueva perspectiva en la composición de formas cuadráticas (los Cubos de Bhargava, ver [1]).

(b) Podemos pensar en $\mathcal{H}_F \subseteq F$ como un subconjunto del plano, ya sea directamente cuando F es imaginario, o mediante la incrustación $\rho : F \hookrightarrow \mathbb{R}^2$ cuando es real. Por tanto, podemos ver $\mathcal{H}_F/\ \mathrm{SL}_2(\mathbb{Z})$ como la manifestación geométrica del grupo de clases estrictas de ideales.

Conclusiones

En este trabajo hemos podido comprobar que, a pesar de no ser la teoría de números algebraica la rama más importante dentro de la teoría de números, sí nos permite obtener resultados potentes. Como se ha mencionado en el trabajo, los resultados acerca de factorización en anillos de enteros cuadráticos permitieron dar un gran salto en la resolución de uno de los problemas más famosos de la Historia de las matemáticas, como es el Último Teorema de Fermat. Fueron estos resultados los que motivaron el estudio de la aritmética en los cuerpos cuadráticos.

Las herramientas algebraicas y analíticas se alternan y complementan para conseguir resultados en Teoría de Números. Y aunque la teoría analítica de números es la más importante dentro de ésta, la teoría algebraica también presenta resultados de gran relevancia.

Personalmente, el tema me ha sorprendido, ya que hasta el momento de iniciar el trabajo ni siquiera me había planteado la posible utilidad de estudiar la aritmética en cuerpos más grandes que $\mathbb{Q}$. Además, cuando conocí el tema, no imaginé que se fueran a poder obtener unos resultados como los dos resultados principales del trabajo. Por una parte, el hecho de contemplar la idea de trabajar la factorización de conjuntos de números, como son los ideales, y comprobar que efectivamente se factorizan de manera única. Por otra parte, la existencia del grupo de clases de ideales, un grupo finito que marca lo lejos que está un anillo de enteros cuadráticos de ser un dominio de factorización única. Creo que fueron dos golpes de genialidad por parte de Kummer que permitieron avanzar en el estudio de la aritmética de los cuerpos cuadráticos.

Ambos resultados nos permiten concluir que no siempre podemos asumir las propiedades de factorización de $\mathbb{Z}$ en los anillos de enteros cuadráticos, pero al mismo tiempo, nunca se estará demasiado lejos de tener factorización única (debido a la finitud del grupo de clases de ideales). Además, en todos los casos podemos recuperar la factorización única trabajando con ideales.

Una vez concluido este trabajo, su continuación natural es el estudio de las formas cuadráticas y su relación con la aritmética en cuerpos cuadráticos. Este tema recuperó relevancia en 2004, cuando Manjul Bhargava presentó un nuevo modo de interpretar las composiciones de formas: los cubos de Bhargava. También es natural la continuación de este estudio con la aritmética en cuerpos formados por la extensión de los racionales mediante una raíz de un polinomio irreducible de grado mayor que 2. Es curioso comprobar que en este caso, los dos resultados probados para cuerpos cuadráticos también son ciertos.

Referencias

[1] M. Bhargava, *Higher composition laws I: A new view on Gauss composition, and quadratic generalizations*, Ann. Math. (2) 159(1), 217-250, 2004.

[2] David Cox, John Little, Donal O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, 2007.

[3] Enrique de Amo Artero, Manuel Úbeda Flores, *Teoría de funciones analíticas de una variable*, Colección Textos Docentes nº22, Editorial Universidad de Almería, Almería, 2018.

[4] Ángel del Río Mateos, *El reto de Fermat*, Nivola, Tres Cantos, 2005.

[5] Larry C. Groove, *Algebra*, Academic Press, New York, 1983.

[6] Simon Singh, *El enigma de Fermat*, Editorial Planeta, Barcelona, 1998.

[7] Mak Trifković, *Algebraic theory of quadratic numbers*, Springer, New York, 2013.